Symantec Enterprise Security Manager™ Security Update 17 User’s Guide

Release for Symantec ESM 6.0 and 5.5
Windows modules

Symantec ESM Security Update 17 for Windows

031215

Copyright Notice

Trademarks

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
    - Error messages/log files
    - Troubleshooting performed prior to contacting Symantec
    - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Symantec Software License Agreement
Symantec Enterprise Security Manager

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU” OR “YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE “AGREE” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE “I DO NOT AGREE” OR “NO” BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the “Software”) is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a “License Module”) that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module. Permission to use the software to assess Desktop, Server or Network machines does not constitute permission to make additional copies of the Software. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software you are authorized to use on a single machine.
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software to assess no more than the number of Desktop machines set forth under a License Module. “Desktop” means a desktop central processing unit for a single end user;
D. use the Software to assess no more than the number of Server machines set forth under a License Module. “Server” means a central processing unit that acts as a server for other central processing units;
E. use the Software to assess no more than the number of Network machines set forth under a License Module. “Network” means a system comprised of multiple machines, each of which can be assessed over the same network;
F. use the Software in accordance with any written agreement between You and Symantec; and
G. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;
B. use the Software to assess a Desktop, Server or Network machine for which You have not been granted permission under a License Module;
C. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
D. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
E. continue to use a previously issued license key if You have received a new license key for such license, such as with a disk replacement set or an upgraded version of the Software, or in any other instance;
F. continue to use a previous version or copy of the Software after You have installed a disk replacement set, an upgraded version, or other authorized replacement. Upon such replacement, all copies of the prior version must be destroyed;
G. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
H. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor
I. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following

Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified by, the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Chapter 1 Introducing Security Update 17 for Windows

Conventions 19
Symantec ESM modules 19
- Account Information 20
- Account Integrity 20
- Active Directory (Windows 2000/Server 2003) 20
- Backup Integrity 20
- Discovery 20
- Disk Quota (Windows 2000/XP) 20
- Encrypted File System (Windows 2000/XP) 21
- File Attributes 21
- File Watch 21
- Integrated Command Engine (ICE) 21
- Login Parameters 21
- Network Integrity 21
- Object Integrity 22
- OS Patches 22
- Password Strength 22
- Registry 22
- Response 22
- Startup Files 23
- System Auditing 23
- System Product Info 23
- User Files (Windows NT) 23

Chapter 2 Installing the Security Update

System requirements 25
Getting the update 26
Getting ready to install 26
Installing the update 27
- LiveUpdate installation 27
- Manual installation 27

Registering the modules 28
Resolving connection errors 28

Chapter 3 Reviewing policies, modules, and messages

Reviewing policies 29
- Implementing best practice policies 29
- Responding to incidents 30
- Creating and editing your own policies 30
- Sample policies 31
  - Phase policies 31
  - Queries policy 32
- Copying and moving policies 33
- Running policies 33
- Demonstrating security checks 33

Reviewing modules 34
- Enabling and disabling security checks 34
- Specifying options 34
- Editing name lists 35
  - Users and Groups name list precedence 36
- Creating and editing templates 37
  - Creating a template 37
  - Editing template rows 38
  - Editing template fields 39

Reviewing messages 40
- Reviewing message types 40
- Reporting duplicate records 41
- Reviewing common messages 41
- Correcting agents in messages 42
- Updating template and snapshot files in messages 42
- Editing messages 43

Chapter 4 Modules

Account Information 45
- Security groups and their users 45
- Users and their security groups 46
- User rights for accounts 46
- Users with administrator privilege 47
- Locked out accounts 47
- Disabled accounts 48
- Expired accounts (Windows NT/2000) 49
- User information 49
- User information (cont’d) 50
- File/folder access for accounts 50
- File/folder access for accounts (cont’d) 51
- Share permissions 52

Account Integrity 53
Account naming conventions 53
ADS account names (Windows 2000) 53
Non-ADS account names 53
Users to check 53
Full/Display name and description required (Windows 2000/Server 2003) 54
Full name and description required (Windows XP) 54
Full name and description required (Windows NT) 55
Rename administrator account 55
Rename guest account 56
Groups guest belongs to 57
Accounts without time restrictions (Windows NT/2000/Server 2003) 58
Accounts without workstation restrictions (Windows NT/2000/Server 2003) 59
Accounts that never expire (Windows NT/2000/Server 2003) 60
Excessive number of accounts 60
Disabled/expired/locked accounts 61
Accounts that must be disabled 62
New users 63
Deleted users 64
Changed users 64
New groups 66
Deleted groups 67
Changed groups 67
User rights checks 69
Access this computer from network 69
Act as part of the operating system 70
Adjust memory quotas for a process (Windows XP/Server 2003) 71
Add workstations to domain (Windows NT/2000/Server 2003) 71
Allow logon through Terminal Services (Windows XP) 72
Back up files and directories 72
Bypass traverse checking 73
Change the system time 74
Create a pagefile 74
Create a token object 75
Create permanent shared objects 75
Debug programs 76
Deny access to this computer from the network (Windows 2000/XP/Server 2003) 76
Deny logon as a batch job (Windows 2000/XP/Server 2003) 77
Deny logon as a service (Windows 2000/XP/Server 2003) 78

Deny logon locally (Windows 2000/XP/Server 2003) 78
Deny logon through Terminal Service (Windows XP/Server 2003) 79
Enable computer and user accounts to be trusted for delegation (Windows 2000/Server 2003) 79
Force shutdown from a remote system 80
Generate security audits 81
Increase quotas (Windows NT/2000/Server 2003) 81
Increase scheduling priority 82
Load and unload device drivers 82
Lock pages in memory (Windows NT) 83
Log on as a batch job 83
Log on as a service 84
Log on locally 85
Manage auditing and security log 85
Modify firmware environment values 86
Perform volume maintenance tasks (Windows XP) 86
Profile single process 87
Profile system performance 88
Remove computer from docking station (Windows 2000/XP/ Server 2003) 88
Replace a process level token 89
Restore files and directories 89
Shut down the system 90
Synchronize directory service data (Windows 2000/Server 2003) 90
Take ownership of files or other objects 91
Create global objects (Windows 2000/XP/Server 2003) 92
Impersonate a client for authentication (Windows 2000/XP/ Server 2003) 92
Active Directory (Windows 2000/Server 2003) 92
Computers with applied GPOs (Windows 2000/Server 2003) 92
Computers without applied GPOs (Windows 2000/Server 2003) 93
Users with applied GPOs (Windows 2000/Server 2003) 93
Users without applied GPOs (Windows 2000/Server 2003) 93
Security groups with applied GPOs (Windows 2000/Server 2003) 94
Security groups without applied GPOs (Windows 2000/ Server 2003) 94
Backup Integrity 95
Backups needed 95
Folders excluded 96
Discovery 96
Targets 96
Symantec ESM device status 97
Symantec Intruder Alert device status 99

- Report if found 100
- Profile candidate devices 100
- Profile timeout 101
- Scan non-responding addresses 101

Disk Quota (Windows 2000/XP) 102

- Volume quota not supported (Windows 2000/XP) 102
- Volume quota disabled (Windows 2000/XP) 103
- Volume quota not enforced (Windows 2000/XP) 103
- Volume quota enforced (Windows 2000/XP) 104
- Volume quota exceeds limit (Windows 2000/XP) 105
- Volume warning exceeds limit (Windows 2000/XP) 105
- Volume quota not logged (Windows 2000/XP) 106
- Volume warning not logged (Windows 2000/XP) 107
- User quota not enforced (Windows 2000/XP) 107
- User exceeds quota (Windows 2000/XP) 108
- User exceeds warning (Windows 2000/XP) 109

Encrypted File System (Windows 2000/XP) 110

- EFS not supported (Windows 2000/XP) 110
- Percentage of encrypted files (Windows 2000/XP) 111
- Files can be decrypted by others (Windows 2000/XP) 111
- File recovery agents not authorized (Windows 2000/XP) 112

File Attributes 113

- Common File Attributes messages 113
- Template file list 114
- Editing the File template 115
  - Editing a Permissions ACL sublist 118
  - Editing an Auditing ACL sublist 120
- Keywords list 121
- Editing the File Keywords template 122
- File ownership 123
- File attributes 125
- Changed file (times) 126
- Changed file (size) 127
- Changed file (signature) 128
- File ACL 129
- Hidden files and folders 131
- File and folder permissions 132
- Files giving all users Full Control 133
- Allow any privileged account 134
- Do not notify if file permissions are increased in security 134
- Do not notify if User/Group in ACL is not on system 134

File Watch 135
- Common File Watch messages 135
- Files/directories to watch 136
  - Editing the File Watch template 136
- Changed files (ownership) 139
- Changed files (signature) 139
  - Editing the File Signatures template 141
- New files 143
- Removed files 144
- Malicious files 145
  - Editing Malicious File Watch templates 146
- Invalid signature 152
- Integrated Command Engine (ICE) 153

Login Parameters 153
- Account lockout threshold 153
- Account lockout duration 155
- Bad logon counter reset 156
  - Legal notice text 157
- Expired logon hours disconnect (Windows NT/2000) 158
- Last user name hidden 159
- Shutdown without logon 160
- Autologon disabled 161
- Inactive accounts 161
- Inactive account timeout (Windows 2000/XP/Server 2003) 162

Network Integrity 163
- Trusted domains (Windows NT/2000) 163
- Local groups 164
- Shared folders 164
- Shared folders giving all users Full Control 165
- Shared printers 166
- Share permissions 167
- Hidden shares 168
- Anonymous LanMan access disabled 168
- Permitted TCP ports 169
- Permitted UDP ports 170
- Permitted IP protocols 171
- Plain text authentication 171
- File security more restrictive than share security 172
- RRAS enabled (Windows 2000/XP) 173
- RAS enabled (Windows NT) 174
- RAS installed (Windows NT) 174
- RRAS requires account callbacks (Windows 2000/XP) 175
- RAS requires account callbacks (Windows NT) 176

RRAS requires preset number for callback (Windows 2000/XP) 177
RAS requires preset number for callback (Windows NT) 177
RRAS NetBIOS gateway disabled (Windows 2000/XP) 178
RAS NetBIOS gateway disabled (Windows NT) 179
RAS encrypted password (Windows NT) 179
RAS authentication retries (Windows NT) 180
RAS authentication time limit (Windows NT) 181
RAS NetBIOS auditing (Windows NT) 181
RAS auditing (Windows NT) 182
RAS encrypted data (Windows NT) 183
Listening TCP ports 184
Listening UDP ports 184
New listening TCP ports 185
Deleted listening TCP ports 186
New network shares 186
Modified network shares 187
Deleted network shares 188
LanMan authentication (Windows NT) 188
New listening UDP ports 189
Deleted listening UDP ports 190
Object Integrity 191
Volumes without ACL control 191
Local accounts 192
OS Patches 193
Application patches 193
Editing the Patch template 193
Comparison operators 197
Patch Keywords templates 198
Editing the Patch Keywords template 198
Common Patch module messages 200
Patch templates 201
Comparisons 201
File versions 202
File dates 202
Registry keys 202
Relaxed 203
Strict 203
Superseded 203
Disable module 203
Internet advisory resources 204

Password Strength ... 204
  How to secure your passwords ... 205
  Users to check ... 205
  Minimum password length ... 205
  Accounts without passwords ... 206
  Password = username ... 207
  Password = any username ... 208
  Password = wordlist word ... 208
    Wordlist files ... 209
  MD4 hashes ... 211
  Reverse order ... 212
  Double occurrences ... 213
  Plural forms ... 214
  Prefix ... 215
  Suffix ... 216
  Password changes ... 217
  Password must expire ... 217
  Maximum password age ... 218
  Minimum password age ... 218
  Password uniqueness ... 219
  Syskey encryption ... 219
Registry ... 220
  Common Registry messages ... 220
  Using wildcard characters ... 221
  Template file list ... 221
  Editing the Registry template ... 222
    Editing an ACL sublist ... 225
    Editing a Snapshot Values sublist ... 226
    Editing a Check Values sublist ... 227
    Editing a Value Info Queries sublist ... 228
    Editing a Data Existence sublist ... 229
    Editing a Skip Conditions sublist ... 230
    Using regular expressions ... 231
    Editing an Auditing sublist ... 234
  Key ownership ... 235
  Key permissions ... 236
  Key and value existence ... 236
  Changed key (time) ... 238
  Changed value (size) ... 238
  Changed value (signature) ... 239
Response ... 239

Startup Files 239
- Installed services 240
- Required services 240
- Disallowed services 241
- Unknown services 242
- Changed services 243
- New services 244
- Deleted services 244
- Services using system account to run 245
- Services using specified user accounts to run 246
- Contents of Run keys 246
- Remote Procedure Call (RPC) disabled 247
- Remote registry access 248
- Remote registry access (anonymous) (Windows NT) 248
- Remote registry access (non-Administrators) (Windows NT) 249

Symantec Product Info 250
- Minimum version (Norton AntiVirus) 251
- LiveUpdate frequency (Norton AntiVirus) 251
- Scan frequency (Norton AntiVirus) 252
- Minimum version (Symantec AntiVirus Corporate Edition) 252
- LiveUpdate frequency (Symantec AntiVirus Corporate Edition) 252
- Scan frequency (Symantec AntiVirus Corporate Edition) 253

System Auditing 253
- Security events success auditing 254
- Security events failure auditing 255
- Security events do not overwrite security log 256
- System halts when security log full 256
- Security event log size 257
- Days until security events are overwritten 258

User Files (Windows NT) 259
- Users to check (Windows NT) 259
- Disable Run on File menu (Windows NT) 259
- Disable Saved/Never Save (Windows NT) 260
- Common program groups (Windows NT) 261
- Script ownership/access (Windows NT) 261
- Script file extensions 263
- Home folder ownership/access (Windows NT) 263
- Suspicious files in folder (Windows NT) 264
- Logon script required (Windows NT) 265

Appendix A Integrated Command Engine (ICE)

Introducing ICE 267
Integrating a new function 268
Creating an ICE template 269
Applying ICE message options 274
    Script Missing messages 274
    Unmapped messages 275
    Message Maps sublist 276
    Report all stderr messages 277
    Redirect stderr to stdout 277
    Return code 277
    Passed messages 278
    Failed messages 279
    Not Applicable messages 280
    Not Available messages 281
    User messages 282

Index

Chapter 1

Introducing Security Update 17 for Windows

This chapter includes the following topics:

- Conventions
- Symantec ESM modules

Conventions

Each chapter in this guide begins with a list such as the one above. In the PDF version, you can click a topic in the list above to go directly to that topic. Similarly, you can click an item in the Contents or Index or a cross-reference that contains a page number.

Most modules run on all Windows operating systems. Those that do not, list the operating systems that they do run on in parentheses after the module name. For example, User Files (Windows NT) runs only on Windows NT.

Symantec ESM modules

A module is an executable file that examines a server or operating system where a Symantec ESM agent is installed. Each module contains security checks and options that assess agent vulnerability to unauthorized access, tampering, and denial of service attacks.

For example, the Login Parameters module includes checks for excessive login failures, expired passwords, and so on. Each check examines a specific area of concern such as inactive accounts or password length.

Account Information

The Account Information module reports requested account information, such as a list of locked out accounts, account folder permissions, or users in specified security groups. See "Account Information" on page 45.

Account Integrity

The Account Integrity module reports new, changed, and deleted accounts, user rights, and vulnerabilities of account names and rights. See "Account Integrity" on page 53.

Active Directory (Windows 2000/Server 2003)

The Active Directory module reports group policy objects (GPOs) that apply to users, groups, and computers in the Active Directory Service (ADS). GPOs are active directory objects that contain group policies such as the security policy. GPO settings can be applied to sites, domains, and organizational units. See "Active Directory (Windows 2000/Server 2003)" on page 92.

Backup Integrity

The Backup Integrity module reports files and folders on local drives that have not been backed up since they were last changed. Backups prevent data loss in the event of a disk or system failure. See "Backup Integrity" on page 95.

Discovery

The Discovery module examines TCP/IP ports in the agent's licensed address class and reports computers running an operating system that is supported by Symantec ESM or Symantec Intruder Alert, and that are not running these products. This helps ensure that all computers that are eligible for these programs are covered. See "Discovery" on page 96.

Disk Quota (Windows 2000/XP)

The Disk Quota module reports how disk quota information is tracked on the computer and reports a problem if it is not tracked. See "Disk Quota (Windows 2000/XP)" on page 102.

Encrypted File System (Windows 2000/XP)

The Encrypted File System module reports whether the Encrypted File System (EFS) is not supported or not being used. It also reports different aspects of the EFS configuration. See "Encrypted File System (Windows 2000/XP)" on page 110.

File Attributes

Security checks in the File Attributes module compare current settings with New File template records and report changes in file ownership, size, creation time, and modification. The module also reports changes in access control lists (ACLs), results of checksum checks, and folders for which the Everyone group has full control permissions. See "File Attributes" on page 113.

File Watch

Security checks in the File Watch module compare current settings with File Watch template records and report changes to files and folders, verify file signatures, and warn of known attack signatures. See "File Watch" on page 135.

Integrated Command Engine (ICE)

The Integrated Command Engine (ICE) is a unique, extensible module in the Dynamic Assessment policy. It contains no security checks or templates, but gives users the ability to integrate user scripts and executables and with Symantec ESM. In effect, they become the module's security checks. Because the ICE module is so different from all other modules, it is documented in the Appendix. See "Integrated Command Engine (ICE)" on page 267.

Login Parameters

The Login Parameters module reports whether the previous user name is displayed on the Logon screen, if shutdown is possible without logon, and if automatic logons are allowed. It also reports old or unused accounts and accounts that are not locked out after a specified number of failed logon attempts. "Login Parameters" on page 153

Network Integrity

The Network Integrity module reports the vulnerabilities of domains, including global security groups and folder and printer shares. The module also reports CD-ROM and floppy disk drives that can be accessed by network users. It evaluates Microsoft's Routing and Remote Access Service (RRAS), which is called Remote Access Service (RAS) on Windows NT. See “Network Integrity” on page 163.

Object Integrity

The Object Integrity module examines ACL support for changes in ownership, permissions, the logical-name table, rights identifiers, and other software objects or device-specific files in the system device directory. The module also detects new devices, deleted devices, and device changes between policy runs. See “Object Integrity” on page 191.

OS Patches

This module searches for operating system patches that have been released for Windows by Microsoft Corporation. The module reports patches that have been released but are not installed as well as patches that are pending release by Microsoft. The Patch template defines patches that are checked and messages that are used to report vulnerabilities. See “OS Patches” on page 193.

Password Strength

The Password Strength module reports passwords that do not conform to specified format, length, and expiration requirements. It also applies dictionary tests to detect passwords that are easily guessed. See “Password Strength” on page 204.

Registry

Security checks in the Registry module compare current settings with Registry template records and report changes in registry key ownership, registry keys and values, and last write times of registry keys. See “Registry” on page 220.

Response

The Response module detects vulnerabilities using templates in Symantec ESM response policies. Response policies are configured by the Symantec Security Response team to respond quickly to new security incidents and vulnerabilities between regular Symantec ESM Security Update releases. Response module templates cannot be created or edited by Symantec ESM users.

Startup Files

The Startup Files module reports information about system services, run keys, and remote registry access. See “Startup Files” on page 239.

System Auditing

System auditing helps you identify unauthorized users and provides valuable tracking information during or after a break-in. This module reports security events that are audited for failure or success and what happens when the log file is full. See “System Auditing” on page 253.

System Product Info

The Symantec Product Info module reports a problem if Symantec AntiVirus Corporate Edition or Norton AntiVirus is not installed on the agent. It also reports a problem if their version number, last scan time, or last LiveUpdate time are not within the limits that you specify. See “Symantec Product Info” on page 250.

User Files (Windows NT)

The User Files module reports suspicious files in user directories, hidden directories, special device files, and mount points in other areas. It also reports file ownerships and permissions that do not match the original baselines. See “User Files (Windows NT)” on page 259.

Chapter 2

Installing the Security Update

This chapter includes the following topics:

- System requirements
- Getting the update
- Getting ready to install
- Installing the update
- Registering the modules
- Resolving connection errors

System requirements

SU17 installation requires the following free disk space:

Agent operating system	Disk space
Windows Server 2003	24 MB
Windows XP Professional (Intel)	24 MB
Windows 2000 Professional or Server (Intel)	26 MB
Windows NT (Intel)	23 MB
AIX	82 MB
Digital UNIX/Tru64/OSF1	66 MB
HP-UX	62 MB

Agent operating system	Disk space
IRIX	87 MB
Red Hat Linux	28 MB
Solaris	52 MB
Sequent	45 MB

The LiveUpdate installation of SU17 for all supported operating systems requires approximately 520 MB per manager.

Getting the update

Symantec ESM Security Updates are available:

- Through LiveUpdate.
  Running LiveUpdate is the standard method of installing Security Updates. Symantec ESM 6.0 or 5.5 upgraded to SU 12 or later is required.
- On the Internet at http://www.symantec.com/downloads.
- On the Security Update CD.
  Two or three times a year, Symantec publishes a set of recent updates on a CD. If you are unable to obtain Security Updates through LiveUpdate and cannot download them from the Symantec Security Response Web site, use the form at the end of this document to order the most recent CD.

Getting ready to install

Before you install the update:

- Ensure that each computer has an installed Symantec ESM agent.
- Prepare a list of all computers that have an installed and running agent that need to be updated.
  Include the names of all managers where each agent is registered.
  Include the Symantec ESM user name, password, and communication protocol that each agent uses to contact the manager.
  The user name and password must have privileges to register agents on the manager.
- Use an account with administrator privileges on the computers where you plan to install the modules.

Installing the update

The standard installation method is to use the LiveUpdate feature in the Symantec ESM console. Another method is to use files from a CD or the Internet to install the policy manually.

Remote security update installations are not supported on Windows operating systems.

LiveUpdate installation

Install the policy by using the LiveUpdate feature in the Symantec ESM console. LiveUpdate installations are automated. See the *Symantec Enterprise Security Manager 6.0 User's Guide* or the *Symantec Enterprise Security Manager 5.5 User Manual*.

Manual installation

If you cannot use LiveUpdate to install the policy directly from a Symantec server, you can install the policy manually, using files from a CD or the Internet.

To install the security update manually

1. Log on as administrator or administrator equivalent.
2. Double-click **esmtpk.exe.**
3. Type **2** to continue with installation.
4. Press **Enter**.
5. The first time you install the Security Update on an operating system, type **Y** to register the template and .m files with the manager.
   On subsequent installations, type **N** to skip the registration. The Security Update only has to be registered with each manager once for each operating system.
6. Press **Enter**.
   If this is the first time you are installing the Security Update on the operating system, and you typed **Y** in step 5, proceed to step 7.
   If this is not the first time you are installing the Security Update on the operating system, and you typed **N** in step 5, this completes the installation.
7. Type the name of the manager that you want to register the template and .m files with.
8. Press **Enter**.
9. Press **Enter** to log on to the manager with the default user name, ESM.

Otherwise, type the name of a user that has the advanced manager right, Register agents with manager.

10 Type the password that gives the user access to the manager.

11 Press **Enter**.

12 Press **Enter** to accept the TCP protocol.

13 Press **Enter** to the accept the default port, 5600.
Otherwise, type the number of the port that you use for Symantec ESM, then press **Enter**.

14 Press **Enter** to use the default name.
Otherwise, type the name of the agent as it is known to the manager, then press **Enter**.

15 Press **Enter** to approve the information that you have entered.

16 When prompted, press **Enter** to exit the installation program.

When an agent is registered to multiple managers, rerun esmtpk.exe on the agent to register the modules with each manager.

Note: Do not register different versions of Symantec ESM agents to the same manager. This can cause manager database errors.

Although agents that were registered to a manager before it was upgraded continue to function with the manager after the upgrade, you should upgrade agents to the same version as the manager.

Registering the modules

Although tuneup packs prompt for a decision to register templates and .m files each time they install security modules on an agent, you do not need to register the updated files more than one time for each manager.

Resolving connection errors

If an agent reports connection errors while running security checks, check the Program Files\Symantec\ESM\config\manager.dat file on the agent.

To resolve connection errors, add the manager's fully-qualified name to the file. If the file is missing, run the esmsetup program to re-register the agent to the manager.

Reviewing policies, modules, and messages

This chapter includes the following topics:

- Reviewing policies
- Reviewing modules
- Reviewing messages

For additional information, see chapter 3 of the *Symantec Enterprise Security Manager 6.0 User's Guide* or chapter of the *Symantec Enterprise Security Manager 5.5 User Manual.*

Reviewing policies

A policy is a set of modules with enabled security checks that report security vulnerabilities.

Symantec ESM is installed with seven sample policies.

Baseline policies and best practice policies can be installed through LiveUpdate or downloaded and installed from the Internet or a CD.

Policies for application products are sold separately.

Implementing best practice policies

Symantec ESM best practice policies are configured to protect specific applications and/or operating systems from security vulnerabilities.

Operating system (OS) hardening policies incorporate Symantec security research based on ISO 17799 and other industry standards and best practices. OS policies can be used in place of the default policies.

OS policies are configured by Symantec with values, name lists, templates, and word files that apply to targeted platforms. They use Security Update modules and templates to check OS patches, password settings, and other vulnerabilities on the operating system. They may also introduce new templates and word lists to examine conditions that are required by supported standards or regulations.

Maintenance-paying Symantec ESM customers can download OS Policies without charge through LiveUpdate or at the Symantec Security Response Web site, http://securityresponse.symantec.com.

Responding to incidents

Maintenance-paying Symantec ESM customers can download Response policies for specific security incidents such as Code Red 2, Nimda, and Blaster without charge at the Symantec Security Response Web site, http://securityresponse.symantec.com.

Creating and editing your own policies

Creating and editing policies requires Create New Policies and Modify Policy access rights. See “Assigning access rights to manager accounts” in your Symantec ESM 6.0 *User’s Guide* or 5.1 or 5.5 *User Manual*.

You can create a new policy (add) or copy (duplicate) an existing policy. After creating a policy, edit it to add or delete modules that the policy runs when it executes.

To add a new policy

1. In the enterprise tree, do one of the following:
   - Right-click a manager, then click **New** > **Policy**.
   - Right-click **Policies**, then click **New Policy**.
2. Type a new policy name of not more than 32 characters.
3. Press **Enter**.

To duplicate a policy

1. In the enterprise tree, right-click a policy, then click **Duplicate**.
2. Type a new policy name of not more than 31 characters.
3. Press **Enter** or click **OK**.

To edit a policy

1. In the enterprise tree, double-click the policy that you want to edit.

2 Edit the name lists:

- In the Available Modules list, click a module that you want to add to the policy, then click the left arrow.
- In the Current Modules list, click a module that you want to remove from the policy, then click the right arrow.

3 Click **OK**.

To rename a policy

1 In the enterprise tree, right-click a policy, then click **Rename**.

2 Type a new policy name of no more than 31 characters.

3 Press **Enter**.

To delete a policy

◆ In the enterprise tree, right-click a policy, then click **Delete**.
The manager must have the Modify Policy access right.
You cannot delete a policy when more than one Symantec ESM console is connected to the manager.
To delete report files that are associated with the policy, delete the /reports/<policy> subfolder in the manager's ESM folder.

Sample policies

Seven sample policies are shipped with Symantec ESM. After installing Symantec ESM, make copies of the sample policies, then rename and edit the copies to implement your company's security policy.

Phase policies

The five phase polices let you begin with the most basic security issues and resolve any weaknesses before proceeding to the next level of complexity.

The policies are:

- Phase 1 policy includes the following modules:
  "Account Integrity" on page 53.
  "Disk Quota (Windows 2000/XP)" on page 102.
  "Encrypted File System (Windows 2000/XP)" on page 110
  "File Watch" on page 135
  "Login Parameters" on page 153.
  "Network Integrity" on page 163.
  "OS Patches" on page 193.
  "Password Strength" on page 204.

“Startup Files” on page 239.
“System Auditing” on page 253.

- Phase 2 policy includes all modules in Phase 1, with more security checks enabled, plus the following modules:
  “File Attributes” on page 113.
  “Object Integrity” on page 191.
  “Registry” on page 220.
  “User Files (Windows NT)” on page 259.

Phase 3 policies let you apply different standards to various networks or computers, such as Relaxed for development or testing, Cautious for production, and Strict for sensitive areas such as finance or strategic planning.

- Phase 3:a Relaxed includes all modules in Phase 2, with more security checks enabled.
- Phase 3:b Cautious includes all modules in Phase 3:a, with more security checks enabled, plus:
  “Backup Integrity” on page 95.
- Phase 3:c Strict includes all modules in Phase 3:b, with more security checks enabled.

Queries policy

The Queries policy reports account information and file permissions. Two modules—File Watch and User Files—are used in both Phase and Queries policies. Queries policy modules are:

- “Account Information” on page 45.
- “Discovery” on page 96.
- “File Watch” on page 135.
- “User Files (Windows NT)” on page 259

Dynamic Assessment policy

The Dynamic Assessment policy integrates your customized scripts and programs with Symantec ESM. It uses one module, Integrated Command Engine (ICE). See “Integrated Command Engine (ICE)” on page 267.

Copying and moving policies

Copying policies ensures that policies are identical on multiple managers.

Moving policies removes a policy from one manager and adds it to another, overwriting any policy-related information on the destination manager.

Copying and moving policies requires the Create New Policies access right. See “Assigning access rights to manager accounts” in the Symantec ESM 6.0 *User’s Guide* or 5.1 or 5.5 *User Manual*.

To copy a policy to another manager

◆ In the enterprise tree, drag and drop a policy on a destination manager.
  You can also right-click a policy, drag and drop it on a destination manager, then click **Copy**.

To move a policy

1. In the enterprise tree, drag the source manager policy and drop it on the destination manager.
2. Click **Move**.

Running policies

To run a policy

◆ In the enterprise tree, do one of the following:
  - Drag and drop your policy on the agent or domain.
  - Drag and drop your agent or domain on the policy.

Demonstrating security checks

Before you apply a new security check to your systems, create a demo policy and add the check to it. Then verify the check on a representative computer. By using a demo policy, you can obtain results without disturbing the settings of policies that are created and named by the Symantec Security Response team.

Delete the demo policy after you complete your demonstrations.

Reviewing modules

A module is a set of security checks and options that looks for security vulnerabilities and reports messages in the console grid.

Enabling and disabling security checks

Only enabled security checks provide information when you run a module.

To enable and disable security checks

1. In the enterprise tree, expand the Policies branch.
2. Expand a module branch.
3. Do one of the following:
   - Double-click a Windows icon.
   - Right-click a Windows icon, then click **Properties**.
4. Do one of the following:
   - Check to enable.
   - Uncheck to disable.

Specifying options

You can control the behavior of security checks with options. Some options contain text fields, where you can specify parameters such as the minimum number of non-alphabetic characters that is required in a password.

Other options are used to specify entities that you want to examine as name lists. For example, in the Users to Check option of the Password Strength module, you specify which users and security groups you want all module security checks to examine or skip. This option is permanently enabled, as indicated by the circle in the box.

To display name lists, click an option or security check on the left side of the window. In name lists that appear on the right side of the window, you can specify items that are included or excluded when you run all or some of the security checks in the module.

Editing name lists

Use name lists to specify items that are included or excluded by all or some of the security checks in a module.

Type	Contents
Users	User account name such as user1 and user2
Groups	User account groups such as system operators and administrators (Windows 2000/XP)
Files/Folders	Files or folders such as C:\Program Files\Symantec\ESM\bin
Enabled/Disabled word files	Word files containing word lists
Enabled/Disabled files	Template files
Key (word)	Sets of keys or keywords
Generic strings	Sets of generic character strings

Some name list panes contain:

- New, Delete, Move Up, and Move Down icon buttons
- List area
- Include and Exclude icon buttons

To add an item to a name list

1. Click **New**.
2. Type the item name.
   You can use the asterisk (*) character as a wildcard character to represent a set of items. For example, \myapp* specifies all files in the \myapp folder.
   To add another item, press **Enter**, then repeat steps 1–2.
3. Click **Include** or **Exclude** to indicate whether to examine or skip the listed items.
4. Click **OK**.

To remove an item from a name list

1. Click the item.
2. Click **Delete**.
3. Click **OK**.

To move an item up or down in a name list

1. Click the item.
2. Click **Move Up** or **Move Down**.
3. Click **OK**.

Users and Groups name list precedence

When a module or security check contains Users and Groups name lists, the names in the Groups list are processed first. Then, within each selected group, names in the Users list are processed.

The following table summarizes the results that you can expect from name lists that include or exclude Users and/or Groups entries:

If the check	And the users list	And the groups list	Then the check reports
Includes a users or groups name list	contains user entries	is blank	Data for all reported users
Includes a users or groups name list	is blank	contains group entries	Data for all reported groups and users that are in them
Excludes a users or groups name list	contains user entries	is blank	Data for all groups and users except the reported users
Excludes a users or groups name list	is blank	contains group entries	Data for all groups except the reported groups and users that are in them
Includes or excludes blank name lists	is blank	is blank	Data for all groups and users

Some modules include Users to check options with name lists that are used by more than one security check. Some of the security checks that use the Users to Check name lists also use their own name lists.

When a security check uses two Users and Groups name lists, the combined contents of the name lists are processed as follows:

If Users to Check option	And check name lists	Then the check reports
Includes Users/ Groups entries	Include Users/Groups entries	Data about all groups and their users, and all users, in both user lists

If Users to Check option	And check name lists	Then the check reports
Includes Users/ Groups entries	Exclude Users/Groups entries that are included by Users to Check	Nothing about groups and users in the check name lists (exclude entries override include entries)
Excludes Users/ Groups entries	Include Users/Groups entries that are excluded by Users to Check	Nothing about groups and users in Users to check name lists (exclude entries override include entries)
Excludes Users/ Groups entries	Exclude Users/Groups entries	Nothing about groups and users that are in the name lists
Includes or excludes blank name lists	Include or Exclude blank name lists	Data for all groups and users

Creating and editing templates

A template is a file that contains module control directives and definitions of objects with their expected states.

The following Windows modules use templates:

- File Attribute. See "Editing the File template" on page 115 and "Editing the File Keywords template" on page 122.
- File Watch. See "Editing the File Watch template" on page 136, "Editing the File Signatures template" on page 141, and "Editing Malicious File Watch templates" on page 146.
- Integrated Command Engine. See "Creating an ICE template" on page 269.
- OS Patches. See "Editing the Patch template" on page 193 and "Editing the File Keywords template" on page 122.
- Registry. See "Editing the Registry template" on page 222.

Warning: If you edit any of the templates that are shipped with Symantec ESM, your changes will be overwritten by the next Security Update. To avoid this problem, create and edit your own templates.

Creating a template

To create a template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. Select an available template type.

3. Type a name for the template without a file extension. Symantec ESM provides the extension based on the template type that you select.
4. Click **OK**.
   Your new template is created in the Templates branch of the enterprise tree with other template files that use the same file extension.

Editing template rows

To edit a template, open it in the Template Editor, add and delete rows, and specify the contents of row fields.

To open a template in the Template Editor

1. In the enterprise tree, expand the Templates branch.
2. Double-click the template that you want to open.

The Template Editor organizes templates into rows and columns. Each row describes a single file, patch, or other item. Columns contain the information that Symantec ESM attempts to match with agent settings.

To add a template row

1. Open a template in the Template Editor, then click **Add Row**.
2. Specify row information, including any sublist information needed.
3. Click **OK** to save the row.
4. Click **Close** to exit the Template Editor.

To remove one or more rows

1. In the Template Editor or Sublist Editor, click the leftmost, numbered button of the row that you want to remove.
   - For a range of rows, hold down the Shift key while you click the first and last row numbers.
   - For multiple non-sequential rows, hold down the Ctrl key while you click the row numbers.
2. Click **Remove Rows**.
3. Click **Save**.
4. Click **Close** to exit the editor.

Editing template fields

In the Template Editor, you can:

- Edit the contents of a string or numeric field.

  String fields can store free-form text such as string fields in the Agent Name, File Name, and File Signature fields of the File Watch template.

  Numeric fields can store positive or negative integers or real (floating point) numbers. The Severity field in the Patch template is an example of a numeric field.

- Check or uncheck a check box.

  Some fields have check boxes that you can check to direct the module to examine specified items, such as the New and Removed check boxes in the File Watch template.

- Select a context menu item.

  Some fields have context menus that are displayed when you click a field, such as Signature fields in File and File Watch templates and Signature Type fields in File Signatures templates.

- Edit a sublist.

  Some fields contain sublists. Sublist fields display the number of items in the sublist (initially, 0). Examples include the OS/Rev columns in File templates and ICE templates.

  Click a numbered sublist button (not a row button) to access the Template Sublist Editor.

  Clicking a sublist button opens the Template Sublist Editor.

  Edit sublist rows in the Template Sublist Editor the same way that you edit template rows in the Template Editor.

Reviewing messages

Messages consist of:

- A message name, in all uppercase. Message names link Symantec ESM code to the text of the message title and must not be changed. Message names appear only in .m files.
- A message title, in mixed case, that is displayed in the console grid. You can edit message titles in .m files. See "Editing messages" on page 43.
- Message text, in mixed case, that is displayed in a separate window of the summary report when you pause your mouse on the Message field in the console grid. You can edit message text in .m files. See "Editing messages" on page 43.
- Class (0–4). Class 0 displays a green message (no action needed), classes 1–3 display yellow messages (needs attention), and class 4 displays a red message (needs immediate attention).
- Some messages display a code in the Updateable/Correctable field of the console grid that identifies the message as template-updateable (TU) or snapshot-updateable (SU). You can click the code to update the template or snapshot file to match the current agent settings. See "Updating template and snapshot files in messages" on page 42.
- Some messages also display a code in the Updateable/Correctable field that identifies the message as correctable (C). You can click the code to reverse agent settings or disable a vulnerable account. See "Correcting agents in messages" on page 42.

Most messages are reported in the console grid, though some common messages are reported in a separate window.

Reviewing message types

Symantec ESM reports four types of messages:

- Common messages, available to all modules, report Symantec ESM operational information such as Correction succeeded, Disk write error, etc.
- Correctable messages reverse current agent settings.
- Updateable messages change template or snapshot settings to the current agent settings.
- Informative messages report administrative information such as lists of user accounts or security vulnerabilities that require manual adjustments.

Reporting duplicate records

Records with identical content are reported in a single message. This eliminates repetition of identical messages.

Reviewing common messages

Several messages that report system conditions are stored in the Program Files\Symantec\ESM\register\<architecture>\common.m file. Some of these common messages are displayed in the console grid, others in separate windows.

The following messages can be generated by more than one module:

Message name	Title	Class
CANCELED	Module execution canceled by user	4
CHECK_NOT_ PERFORMED	Warning - check could not be performed	1
CORRECT_FAIL	Correction failed	0
CORRECT_SUCCEED	Correction succeeded	0
DISK_WRITE_FAIL	Disk write error	0
EOF	End of file	0
FEATURE_NOTSUP	Module feature not supported	0
HEADER	No problems found	0
NOMEM	Failed to allocate memory	4
NOTE	Note	0
SNAPSHOT_CREATED	Snapshot created	4
SYSERR	Unexpected system error	4
TEMPLATE_ITEM	Template item	0
TEMPLATE_SUBLIST	Template sublist item	0
TOOMANYERR	Too many report records, please correct problems and rerun	4
UPDATE_FAIL	Update failed	0
UPDATE_SUCCEED	Update succeeded	0

Correcting agents in messages

Correctable messages display a C in the Updateable/Correctable field of the console grid.

You can use the Correct feature to correct agent rights or settings. For example, in the Account Integrity module, the Generate security audits check reports accounts with rights to generate entries in the security log. If you correct a reported user account, the right is revoked. You can restore the right by repeating the same process that you used to revoke it.

You can also use the Correct feature to disable a vulnerable account. In the Password Strength module, for example, you can immediately disable a reported account that has no password.

To correct the agent reported in the console grid

1. In the console grid, right-click an item that contains C in the Updateable/ Correctable field, then click **Correct**.
2. Type the name and password of a user that has the right to change the setting (usually a member of the Administrators security group).
3. Click **OK**.

To reverse a correction, use the same procedure except in step 1, right-click an item that contains Corrected in the Updateable/Correctable field, then click **Correct**.

Updating template and snapshot files in messages

Some modules use template files that specify authorized settings. When you run a module with enabled checks that examine these settings, discrepancies are reported with a TU code in the console grid.

Similarly, some modules use snapshot files that contain settings that were found the last time the module was run. (The snapshot file is created when you run the module for the first time. Changes are detected in subsequent policy or module runs.) Settings that do not match the snapshot file are reported with a SU code in the console grid.

To update a template or snapshot file in the console grid

1. In the console grid, right-click an item that contains **TU** or **SU** in the Updateable/Correctable field.
2. Click **Update Template** or **Update Snapshot**.

Editing messages

Messages are contained in module initialization files, called .m (dot-m) files. The .m file of each module:

- Specifies security checks and options for the module.
- Associates the module with specified name lists.
- Contains a descriptive name for the module.
- Supplies default values for the module's security checks.
- Supplies message text that is reported in the console grid.

During agent registration, the current version of each .m file is stored in the manager database at \ESM\ register\<operating system>\<module name>.m. You can specify the location of .m files on each agent.

.m files contain ASCII text. Some lines begin with directives—words that are preceded by a period (.)—that classify file information. Directives are usually followed by data and sometimes by descriptive text.

Messages begin with .begin directives, which always occur after information about security checks, options, and templates. Do not delete or reorder any messages.

To edit messages

1. Select an agent with an operating system that reports messages that you want to edit.
2. Open the common.m file or <module>.m file in a text editor.
3. Edit the following directives as needed:

Directive	Description
.title	Brief description of a security problem, enclosed in quotation marks, not exceeding 79 characters. For example, .title “Maximum password age too high” The description is displayed in the console grid when the module runs.
.class	Severity of the problem, 0–4. For example: .class 2 0 = Green message (no action required) 1 = Yellow message (deserves attention) 2 = Yellow message (deserves attention) 3 = Yellow message (deserves attention) 4 = Red message (deserves immediate attention)

Directive	Description
.text	Explanation of the problem. Lines of text cannot exceed 128 characters and the total explanation cannot exceed 1,023 characters. Begin text on the line after the .text directive. Include: ■ Nature of the problem. ■ Why it is a security risk. ■ How to remedy the problem. The .endtext directive should occur on a line by itself after the text (required even if you omit an explanation). For example, .text The maximum password age is set too high. Infrequent password changes allow anyone with a stolen password long term access to your system. Set the maximum password age to 60 days. .endtext **Note:** Do not begin a line of text with a period. This character is used as a control delimiter and improper usage causes the module to fail.

4 Change the .customized directive value of each modified message to 1.
This prevents the edited message from being overwritten when the module is updated to a later version.

5 Increment the module version number in the .module directive by 1. In the following example, 1300 was the last version number:
.module “Account Information” acctinfo 1301 WIN2000.

6 Save the edited .m file.

7 Re-register the module with appropriate managers.

8 Verify that the edited messages appear in the message.dat file on computers in the default location (initially \ESM\system\<system name>\db\message.dat).

Chapter 4

Modules

Account Information

The Account Information module reports account information such as locked out accounts, account folder permissions, and users in specified security groups.

For backward compatibility with applications that require anonymous read access, every user is an implicit member of the Everyone security group. The Everyone group rights are examined as part of the other security group checks.

Security groups and their users

This security check reports user names in each security group.

Message name	Title	Class
GROUP_AND_USER	Security group member	0

To demonstrate the check

1. In a demo policy, disable all Account Information module checks except Security groups and their users.
2. Add a test security group and a test user to the agent computer.
3. Add the test user to the test security group.
4. Delete all entries in the excluded Groups to Check name list.
5. Run the demo policy on the agent.
6. Verify that Security group member is reported.

To protect your computers

- Remove users that are not authorized members of security groups.

Users and their security groups

This security check reports specified users and the security groups that they belong to.

Message name	Title	Class
USER_AND_GROUP	User’s security group	0

To demonstrate the check

1. In a demo policy, disable all Account Information module checks except Users and their security groups.
2. Add a test security group and a test user to the agent computer.
3. Add the test user to the security group.
4. In the check’s User name list, add the test user.
5. Check Include these Users/Groups.
6. Run the demo policy on the agent.
7. Verify that User’s security group is reported.

To protect your computers

- Delete unauthorized groups and users.

User rights for accounts

This security check reports the rights granted to each user account and indicates whether they were granted directly or through global or local security group memberships.

Message name	Title	Class
RIGHTS_OF_USER	User right	0

To demonstrate the check

1. In a demo policy, disable all Account Information module checks except User rights for accounts.
2. Add a test security group and a test user to the agent computer.
3. Add the test user to the test security group.
4. Grant the Access this computer from the network right to the test security group.

5. Delete all entries in the Users and Groups name lists.
6. Run the demo policy on the agent.
7. Verify that User right is reported.

To protect your computers

- Remove any rights that have been assigned to users without authorization.

Users with administrator privilege

This security check reports the names of users in the Administrators security group. These users have complete control of the Windows environment.

Message name	Title	Class
USERS_WITH_ ADMIN	Users with administrator privileges	0

To demonstrate the check

1. In a demo policy, disable all Account Information module checks except Users with administrator privilege.
2. Add a test user to the agent computer.
3. Add the test user to the Administrators security group.
4. Delete all entries in the Users and Groups name lists.
5. Run the demo policy on the agent.
6. Verify that Users with administrator privileges is reported.

To protect your computers

- Remove any Administrator rights that have been assigned to users without authorization.

Locked out accounts

This security check reports locked out accounts on the computer.

Message name	Title	Class
LOCKED_OUT_ACCOUNTS	Locked out account	0

To demonstrate the check

1. In a demo policy, disable all Account Information module checks except Locked out accounts.

2 Add a test user to the agent computer.

3 Set the test user account to be locked out after one failed logon attempt.

4 Make two failed logon attempts on the test user account.

5 Remove all entries in the Users and Groups name lists.

6 Run the demo policy on the agent.

7 Verify that Locked out account is reported.

To protect your computers

◆ Contact the user to see if the lockout was due to a forgotten password or an intruder, then take appropriate action.

Disabled accounts

This check lists disabled accounts on the computer. Use the name lists in the check to exclude or include specified users and security groups. See "Editing name lists" on page 35.

Message name	Title	Class
DISABLED	Disabled account	0

To demonstrate the check

1 Disable all Account Information module checks in a demo policy except Disabled accounts.

2 Add a test user to the agent computer.

3 Disable the test user account.

4 In the Disabled accounts check, remove all entries in the Users and Groups name lists.

5 Run the demo policy on the agent.

6 Verify that Disabled account is reported.

To protect your computers

◆ Remove any disabled accounts that are not needed and reactivate those that are needed.

Expired accounts (Windows NT/2000)

This security check reports expired accounts on domain controllers. Expired accounts on Windows 2000 Professional systems and member servers are not reported.

Message name	Title	Class
EXPIRED_ACCOUNTS	Expired account	0

To demonstrate the check

1. In a demo policy, disable all checks in the Account Information module except Expired accounts.
2. Add a test user to an agent computer.
3. Set the test user account to expire.
4. Remove all entries in the Users and Groups name lists.
5. When the account expires, Run the demo policy on the agent.
6. Verify that Expired account is reported.

To protect your computers

- Delete any expired accounts.

User information

This security check reports selected account policy settings.

Enable the User information (cont'd) option to specify policy settings that are to be reported. Use the name lists in the check to exclude or include specified users and security groups.

Message name	Title	Class
USER_INFO	User information	0

To demonstrate the check

1. In a demo policy, disable all checks in the Account Information module except User information.
2. Add a test user to an agent computer.
3. Disable the test user account.
4. Delete any entries in the Users and Groups name lists.

5. In the User information (cont'd) option, disable all listed keys except Disabled account.
6. Run the demo policy on the agent.
7. Verify that the disabled account policy setting is reported in the User information message.

To protect your computers

- Review reported user information for anomalies.

User information (cont'd)

This option lists policy settings that you can enable for the User information security check. These policies can be enabled and disabled:

Account never expires	Password is expired
Description	Password last changed
Disabled account	Password never expires
Expiration date	Password not required
Expired account	Profile path
Logon script name	User can't change password
Locked out account	

File/folder access for accounts

This security check reports the access rights of users and security groups to all files in the specified folder and subfolders.

Use the check's name list to specify the folder to be examined. If the specified folder contains subfolders, the subfolders are also examined.

Use the name lists in the File/folder access for accounts (cont'd) option to exclude or include specified users or security groups.

Message name	Title	Class
DIR_ACCESS	Account with folder permissions	0
FILE_ACCESS	Account with file permissions	0
FILE_LOCKED	Locked file	0

To demonstrate the check

1. In a demo policy, disable all checks in the Account Information module except File/folder access for accounts.
2. Add a test user to an agent computer.
3. Add a test folder to an NTFS volume on the agent computer.
4. Add a test file to the test folder.
5. Produce the following messages:

Message name	Steps
Account with file permissions	1 Assign read and write file permissions to the test user for the test file. 2 In the File/folder access for accounts check, add the path of the test file to the Folders to Check name list. 3 In the File/folder access for accounts (cont'd) option, delete all entries in the Users and Groups name lists. 4 Run the demo policy on the agent. 5 Verify that Account with file permissions is reported.
Account with folder permissions	1 Assign read and write folder permissions to the test user for the demo policy. 2 In the File/folder access for accounts check, add the path of the test file to the Folders to Check name list. 3 In the File/folder access for accounts (cont'd) option, delete all entries in the Users and Groups name lists. 4 Run the demo policy on the agent. 5 Verify that Account with folder permissions is reported.

A Locked file message is reported when another service locks the file. To obtain information about the file, stop the other service.

To protect your computers

- Review reported anomalies and take appropriate action.

File/folder access for accounts (cont'd)

Use this option to specify users and security groups that are not to be reported by the File/folder access for accounts check. The default name lists exclude the %Administrator% and %System% users and the %Administrators% security group.

Share permissions

This security check reports accounts that can access file/folder shares, including the account, file or folder, access permissions, and file or directory path.

Use the name lists in the check to exclude or include specified users and security groups.

The check returns the following message:

Message name	Title	Class
SHARE_PERMISSIONS	Account with share permissions	0

To demonstrate the check

1. In a demo policy, disable all checks in the Account Information module except Share permissions.
2. Add a test user to an agent computer.
3. Add a test folder to a volume on the agent computer.
4. Share the test folder.
5. Grant the test user access through share permissions.
6. Delete any entries in the name lists.
7. Run the demo policy on the agent.
8. Verify that Account with share permissions is reported.

To protect your computers

- ◆ Review the report for anomalies.

Account Integrity

The Account Integrity module reports new, changed, and deleted accounts, account name and rights vulnerabilities, and user rights.

Many module checks are correctable and/or updateable. See "Correcting agents in messages" on page 42 and "Updating template and snapshot files in messages" on page 42.

Account naming conventions

ADS account names (Windows 2000)

On a Windows 2000 server running as an ADS domain controller, user and group (account) names are reported as a DNS-style domain name followed by an account path. Forward slashes separate path items. For example, in network domain mydept.mycompany.com, user john doe is: mydept.mycompany.com/users/john doe.

Note: User common names, not logon names are reported.

The default location of most accounts in the domain tree is the .../users folder. Some standard groups are in the .../builtin folder.

System administrators can create new folder and change default account folders. The module looks for accounts in all domain folders.

Non-ADS account names

For non-ADS operating systems, account names are reported in the Windows NT format. For example, ExampleDomain\Username.

On Windows NT 4.0, three well-known groups are represented as foreign security principal objects in the .../foreignsecurityprincipals folder:

- Everyone
- NT AUTHORITY\Authenticated Users
- NT AUTHORITY\INTERACTIVE

Users to check

Use this option to exclude or include users or security groups for all checks in the Account Integrity module. See "Editing name lists" on page 35.

Full/Display name and description required (Windows 2000/Server 2003)

For systems with ADS, this security check reports users that do not have entries in the Display name or Description fields of the user’s Properties dialog box.

For systems that are not running ADS, the check reports users that do not have entries in the Full name or Description fields.

Use the name lists in the check to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
FULL_NAME	Full/Display name or description not provided	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Full/Display name and description required.
2. Add a test user. Do not enter the user’s full/display name and/or description in the user Properties dialog box.
3. Run the demo policy on the agent.
4. Verify that Full/Display name or Description not provided is displayed.

To protect your computers

◆ Enter a full name and description for all user accounts.

Full name and description required (Windows XP)

This security check reports users that do not have entries in the Full name or Description fields of the user’s Properties dialog box. All accounts should have entries in these fields to clarify account ownership.

You can use the name list to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
FULL_NAME	Full/Display name or Description not provided	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Full name and description required.
2. Add a test user. Do not enter the user's full name and/or description in the user Properties dialog box.
3. Run the demo policy on the agent.
4. Verify that Full/Display name or Description not provided is displayed.

To protect your computers

- ◆ Enter a full name and description for all user accounts.

Full name and description required (Windows NT)

This security check reports users that do not have entries in the Full name or Description fields of the user's Properties dialog box.

You can use the name list to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
FULL_NAME	Full name or Description not provided	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Full name and description required.
2. Add a test user. Do not enter the user's full name and/or description in the user Properties dialog box.
3. Run the demo policy on the agent.
4. Verify that Full/Display name or Description not provided is displayed.

To protect your computers

- ◆ Enter a full name and description for all user accounts.

Rename administrator account

This security check reports accounts that are named Administrator or any other name that you specify in the name list.

The Administrator account name is well known. For this reason, it can become the target of break-in attempts. Unlike other accounts, Windows does not lock out this account during repeated break-in attempts.

The check returns the following message:

Message name	Title	Class
RENAME_ ADMINISTRATOR	Rename administrator account	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Rename administrator account.
2. Verify that an account with the Administrator account name exists on the demo agent computer.
3. Confirm that the Users name list in the check contains the administrator account name that you want to be reported.
   To report the message for a renamed administrator account, add the new name to the name list before running the policy.
4. Run the demo policy on the agent.
5. Verify that Rename administrator account is reported.

To protect your computers

◆ Rename the administrator account.

Rename guest account

This security check reports any accounts that are named Guest, or any other name that you specify in the name list.

If the guest account is enabled and a password has not been assigned, anyone can access the system. This creates two major security problems:

- By default, Windows assigns Full Control rights to all new file shares. If these permissions are not changed, anyone accessing the system with a guest account has full control over the shared files.
- Many registry keys are readable and writable by members of the Everyone security group, including guest. If these permissions are not changed, anyone accessing the system with a guest account can overwrite these registry keys.

The check returns the following message:

Message name	Title	Class
RENAME_GUEST	Rename guest account	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Rename guest account.
2. Confirm that the Users name list in the check contains the guest name entry.
   To report the message for a renamed guest account, add the new name to the name list before running the policy.
3. Run the demo policy on the agent.
4. Verify that Rename guest account is reported.
   To report the message for a renamed guest account, add the new name to the name list before running the policy.

To protect your computers

- Disable the guest account, or rename it and assign a password to it.

Groups guest belongs to

This security check reports security groups that the guest account belongs to. By default, the guest account belongs to the Everyone, Guests, and None security groups.

Note: The None security group name is language-dependent. Verify that this security group is excluded in the check's name list to ensure that the check produces expected results.

If the guest account belongs to security groups other than those specified in your security policy, users logging on to the guest account can gain unauthorized access to the system.

You can use the name lists in the check to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
GUEST_GROUPS	Guest account is a member of unauthorized groups	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Groups guest belongs to.
2. Verify that the %Everyone%, %Guests%, and None security groups are excluded, either by the Users to check option or by the check's name list.
3. Add a local demo security group to an agent computer. Ensure this security group is not excluded by the Users to check option or by the check's name list.
4. Add the guest account to the demo security group.
5. Run the policy on the agent computer.
6. Verify that Guest account is a member of unauthorized groups is reported.

To protect your computers

- Remove the guest account from unauthorized security groups.

Accounts without time restrictions (Windows NT/2000/Server 2003)

This security check for domain controllers reports accounts that are not restricted to specified hours and days.

Accounts without time restrictions can be used to break into the system after business hours. Grant this right only to users and groups that need access beyond normal business hours.

You can use the name lists in the check to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
NO_TIME_RESTRICTIONS	No account time restrictions	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Accounts without time restrictions.
2. Add a test user with the right to log on at all hours to a test agent computer.
3. Run the demo policy on the agent.
4. Verify that No account time restrictions is reported.

To protect your computers

- If the users/groups are authorized for this right, update the template manually.
- If they are not authorized, revoke the right.

Accounts without workstation restrictions (Windows NT/2000/ Server 2003)

This security check for domain controllers reports accounts that can be accessed on any workstation in the domain.

You can use the name lists in the check to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
NO_WORKSTATION_RESTRICTIONS	No workstation restrictions	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Accounts without workstation restrictions.
2. Add a test user with the right to log on to all workstations to a test agent computer.
3. Run the policy on the agent.
4. Verify that No workstation restrictions is reported.

To protect your computers

- Restrict users to specific workstations unless authorized users need additional access.

Accounts that never expire (Windows NT/2000/Server 2003)

This security check for domain controllers reports accounts that never expire.

Temporary workers may require accounts that grant critical rights. You can limit these accounts over time. Accounts for temporary workers that never expire are difficult to administer and can be used for malicious attacks.

You can use the check name lists to exclude users or security groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
ACCOUNT_NEVER_ EXPIRES	Account never expires	TU	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Accounts that never expire.
2. Add a test user to an agent computer.
3. Set the test user account to never expire.
4. Run the demo policy.
5. Verify that Account never expires is reported.

To protect your computers

◆ Do one or more of the following:

- For accounts that are authorized to never expire, update the template.
- For temporary accounts, specify expiration dates in the template.

Excessive number of accounts

This security check reports a problem when more than a specified number of accounts exists.

In the Max accounts text box, type the maximum number of accounts that is authorized for the system. The default value is 3.

Domain controllers and other sensitive systems should have a limited number of user accounts.

The check returns the following message:

Message name	Title	Class
TOO_MANY_ ACCOUNTS	Too many accounts	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Report Excessive Number of Accounts.
2. In the Report Excessive Number of Accounts check, specify 0 (zero) for the maximum number of accounts.
3. Run the demo policy on the agent.
4. Verify that Too many accounts is reported.

To protect your computers

- Limit the number of accounts to a necessary minimum.

Disabled/expired/locked accounts

This security check reports accounts that have been disabled, expired, or locked out for a period longer than a specified period.

Windows does not keep track of the date when it disables, expires, or locks out an account. The Account Integrity module stores the date that it first detects the disabled, expired, or locked out account in the snapshot file. It uses this value to calculate the elapsed time for the account.

Note: This check must be enabled for other checks in the module to report information about disabled, expired, or locked out accounts.

Type the maximum number of days in the Max disabled time (days) text box. The default value is 90.

The check returns the following message:

Message name	Title	Class
DISABLED	Disabled, expired, or locked account	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Disabled/expired/locked accounts.
2. In the Disabled/expired/locked accounts check, set the maximum disabled number of days to 0 (zero).
3. Add a test user to an agent computer.
4. Disable the test user account.
5. Run the demo policy on the agent.
6. Verify that Disabled, expired, or locked account is reported.

To protect your computers

1. Contact the users of disabled, expired, or locked accounts.
2. Reactivate the accounts or delete them from the system.

Accounts that must be disabled

This security check reports accounts that should be disabled, but are not.

You can use the name list to include accounts that are not already included by the Users to check option.

The check returns the following message:

Message name	Title	Class
DISABLED_ ACCOUNT	Account must be disabled	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except Accounts that must be disabled.
2. Add a test user to an agent computer.
3. In the Accounts that must be disabled check, add the name of the test user account to the name list.
4. Run the demo policy on the agent.
5. Verify that Account must be disabled is reported.

To protect your computers

- Remove any disabled accounts that are not required for normal business operations.
- Periodically review accounts that should be disabled to Ensure they are, in fact, disabled.

New users

This security check reports accounts that were added after the last snapshot update.

Windows 2000 and NT domain controllers report new local users and new global group users.

The check returns the following message:

Message name	Title	Type	Class
USER_ADDED	New user	SU	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except New users.
2. If you have never run the module, run it once to create the snapshot file.
3. Add a new test user to an agent computer.
4. Run the demo policy on the agent.
5. Verify that New user is reported.

To protect your computers

1. For authorized accounts, update the snapshot.
2. Delete unauthorized accounts.

Deleted users

This security check reports accounts that were deleted after the last snapshot update.

Windows 2000 and NT domain controllers report deleted local users and deleted global group users.

The check returns the following message:

Message name	Title	Type	Class
USER_DELETED	User deleted	SU	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except New users and Deleted users.
2. If you have never run the module, run it once to create the snapshot file.
3. If you have not already done so, create a test user, then run the demo policy to generate the New user message and update the snapshot. See “New users” on page 63.
4. Delete the test user.
5. Run the demo policy again.
6. Verify that User deleted is reported.

To protect your computers

1. For authorized deletions, update the snapshot.
2. Restore unauthorized deletions.

Changed users

This security check reports accounts that were changed after the last snapshot update. Reported changes include name, home folder, group memberships, and rights.

Windows 2000 and NT domain controllers report changed local users and changed global group users.

The check returns the following messages:

Message name	Title	Type	Class
USER_ADDED_TO_ GROUP	New user in group	SU	1
USER_HOMEDIR_CHANGED	Changed user home folder	SU	1
USER_NAME_ CHANGED	Changed user logon name	SU	1
USER_REMOVED_FROM_GROUP	User removed from group	SU	1
USER_RIGHT_ADDED	User right granted	SU	1
USER_RIGHT_ REMOVED	User right revoked	SU	1

To demonstrate the check

1 In a demo policy, disable all checks in the Account Integrity module except New users and Changed users.

2 If you have never run the module, run it once to create the snapshot file.

3 Add a local demo security group to an agent computer.

4 Produce the following messages:

Message title	Steps
New user in group	1 Add a new test user to a test security group on the agent computer. 2 Run the demo policy on the agent. 3 Verify that New user in group is reported.
Changed user logon name	1 Rename the new test user. 2 Run the demo policy on the agent. 3 Verify that Changed user logon name is reported.
User right granted	1 Add the Access This Computer From Network right to the new test user. 2 Run the demo policy on the agent. 3 Verify that User right granted is reported.
User right revoked	1 Remove the Access this computer from network right from the new test user. 2 Run the demo policy on the agent. 3 Verify that User right revoked is reported.

Message title	Steps
Changed user home folder	1 Change the new test user’s home folder. 2 Run the demo policy on the agent. 3 Verify that Changed user home folder is reported.
User removed from group	1 Remove the new test user from the demo security group. 2 Run the demo policy on the agent. 3 Verify that User removed from group is reported.

To protect your computers

- ◆ Do one of the following:
  - For authorized changes, update the snapshot.
  - For authorized changes, restore the previous settings.

New groups

This security check reports security groups that were added after the last snapshot update.

The check returns the following message:

Message	Title	Type	Class
GROUP_ADDED	New group	SU	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except New groups.
2. If you have never run the module, run it once to create the e file.
3. Add a new test security group to an agent computer.
4. Run the demo policy on the agent.
5. Verify that New group is reported.

To protect your computers

- ◆ Do one of the following:
  - For new authorized security groups, update the snapshot.
  - Delete unauthorized security groups.

Deleted groups

This security check reports security groups that were deleted after the last snapshot update.

The check returns the following message:

Message name	Title	Type	Class
GROUP_DELETED	Group deleted	SU	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except New groups and Deleted groups.
2. If you have never run the module, run it once to create the snapshot file.
3. If you have not already done so, add a test group and update the snapshot.
4. Delete the test group.
5. Run the demo policy on the agent.
6. Verify that Group deleted is reported.

To protect your computers

- Do one of the following:
  - For authorized deletions, update the snapshot.
  - For unauthorized deletions, restore the security groups.

Changed groups

This security check reports security groups that were changed after the last snapshot update.

The check returns the following messages:

Message name	Title	Type	Class
GROUP_MEMBER_ADDED	Group member added	SU	1
GROUP_MEMBER_REMOVED	Group member removed	SU	1
GROUP_NAME_CHANGED	Group name changed	SU	1
GROUP_PRIV_ADDED	Group right granted	SU	1
GROUP_PRIV_REMOVED	Group right revoked	SU	1

To demonstrate the check

1. In a demo policy, disable all checks in the Account Integrity module except New groups and Changed groups.
2. If you have never run the module, run it once to create the snapshot file.
3. Add a test user to the agent computer.
4. Add a test security group to the agent.
5. Run the policy and update the snapshots.
6. Produce the following messages:

Message title	Steps
Group member added	1 Add the new test user to the new demo group. 2 Run the demo policy on the agent. 3 In the console grid, verify that Group member added is reported.
Group member removed	1 Remove the new test user from the test group. 2 Run the demo policy on the agent. 3 In the console grid, verify that Group member removed is reported.
Group name changed	1 Change the group name. 2 Run the demo policy on the agent. 3 In the console grid, verify that Group name changed is reported.
Group right granted	1 Add the Access this computer from network right to the new demo group. 2 Run the demo policy on the agent. 3 In the console grid, verify that Group right granted is reported.
Group right revoked	1 Remove the Access this computer from network right from the new demo group. 2 Run the demo policy on the agent. 3 In the console grid, verify that Group right revoked is reported.

To protect your computers

- Do one of the following:
  - In the console grid, update the snapshot for authorized changes.
  - Reverse unauthorized changes.

User rights checks

This header precedes Account Integrity checks that report accounts with specific user rights assignments. (Even deleted accounts are reported until you use the Correct feature.)

User rights are defined in Windows Security Settings | Local Policies | User Rights Assignment.

Note: When Windows accounts are deleted, associated user rights information is not always deleted. Symantec ESM reports all user rights that it finds, including those for deleted accounts. To remove user rights information from deleted accounts, use the Correct feature in the Updateable/Correctable field.

To demonstrate user rights checks

1. In a demo policy, disable all checks in the Account Integrity module except the check you are demonstrating.
2. Add a test user to the agent computer.
3. Grant the test user the user right that corresponds to the check.
4. Verify that the test user is not excluded by the name lists in the check or in the Users to check option.
5. Run the demo policy on the agent.
6. Verify that appropriate the message is reported.

Access this computer from network

This security check reports accounts that can access the computer from the network.

Users should authenticate their domain accounts through a domain controller before gaining access to resources on the network.

Users that have this right by default vary according to the Windows version:

Professional	Server	Domain controller
Administrators	Administrators	Administrator
Backup Operators	Backup Operators	Authenticated User
Power Users	Power Users	Everyone
Users	Users	
Everyone	Everyone	

The check returns the following message:

Message name	Title	Type	Class
ACCESS_FROM_NETWORK	Access this computer from network	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Require Administrators to log on to servers locally.
- Use the Correct feature to revoke this right from unauthorized users.

Act as part of the operating system

This security check reports accounts that have the right to act as part of the operating system. By default, this right is granted only to Windows subsystems. The Local System account always has this right.

The right lets an account act as a trusted part of the operating system with system privileges.

You can use the name lists to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message	Title	Type	Class
ACT_AS_OS	Act as part of the operating system	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Run services that require this user right under the Local System account, which always has this right.
- Do not assign the right to any user or security group.
- Use the Correct feature to revoke this right from unauthorized users.

Adjust memory quotas for a process (Windows XP/Server 2003)

This check reports accounts with rights to increase quotas. Processes running under accounts with this user right can increase the memory quota of other processes. Abuse of this right can deny services to other users.

You can use the name list to exclude or include users or security groups that are not excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Class
INCREASE_QUOTAS	Adjust memory quotas for a process	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- ◆ Grant this right only to members of the Administrators security group.

Add workstations to domain (Windows NT/2000/Server 2003)

This security check reports accounts with rights to add workstations to a domain.

This advanced user right is not given to any user or security group by default and should not be granted to any user unless absolutely required.

Use the name list to exclude or include users or security groups that are not excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
ADD_WORKSTATION	Add workstations to domain	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. Grant the right only to members of the domain Administrators group.

Allow logon through Terminal Services (Windows XP)

This check reports accounts with rights to log on to the system through Terminal Services.

Use the name lists in this check to exclude or include users or groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
LOGON_THROUGH_TERMINAL_SERV	Allow logon through Terminal Services	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users.

Back up files and directories

This security check reports accounts with rights to back up files and directories.

You can use the name lists in the check to exclude or include users or groups that are not already excluded by the Users to check option.

Users that are given this right by default vary according to the version of Windows on the system.

The following users can be given backup rights:

Professional	Server	Domain controller
Administrators Backup operators	Administrators Backup operators	Administrators Backup operators Server operators

The Server Operators group is a local group on Windows domain controllers.

Although users with this right may not be able to read file or directory contents directly, they can move sensitive information to other systems where unauthorized users can access it. Restrict the backup right to members of the Administrators, Backup operators, and Server operators security groups to prevent unauthorized users from circumventing file and folder permissions to obtain read access to files and folders.

The check returns the following message:

Message name	Title	Type	Class
BACKUP	Back up files and directories	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users.

Bypass traverse checking

This security check reports accounts that have the right to bypass traverse checking of files and subdirectories.

By default, this advanced right is given to the Everyone security group. It lets a user account pass through file system or registry folders to which it has no access rights to open subfolders or objects to which it does have access rights.

Revoke this right from the Everyone security group. Then use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
BYPASS_TRAVERSE_CHECK	Bypass traverse checking	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

Change the system time

This security check reports accounts that have the right to set the system time. By default, this right is given to Administrators on workstations and servers, and to Power Users on workstations. It should not be given to other users.

Maintaining an accurate system time is critical to auditing and tracking of unauthorized activities on a system. The right to change system time can be used to circumvent software licensing and other time-based controls.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
SYSTEMTIME	Change the system time	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users.

Create a pagefile

This security check reports accounts with rights to create or change the size of pagefiles. Pagefiles are used to temporarily store portions of the system memory when there is not enough memory for all running applications and services to be loaded simultaneously. Adjusting the pagefile size can affect system performance.

By default, this advanced right is given to the Administrators security group. You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
CREATE_PAGE_FILE	Create a pagefile	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right any user who is not a member of the Administrators security group.

Create a token object

This security check reports accounts with rights to create security access tokens. By default, this advanced right is not given to users. The right is used only by the system, processes, and threads. When a process requires this right, run it under the Local System account, which always has this right.

You can use the name lists in the check to exclude or include users or security groups who are not already included or excluded by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
CREATE_TOKEN	Create a token object	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right for Ensureevery account except Local System.

Create permanent shared objects

This security check reports accounts with rights to create permanent shared objects.

Accounts with this right can create directory objects in the Windows object manager to extend the object name space. The right is normally used only by kernel mode components and is not directly assigned to any users or security groups.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
CREATE_SHARED	Create permanent shared objects	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. Do not grant this right to any user or security group.

Debug programs

This security check reports accounts with rights to debug programs. These accounts can attach a debugger to any process, including critical operating system components and low-level objects such as processes or threads.

This advanced right is given to the Administrators security group by default.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message	Title	Type	Class
DEBUG_PROGRAMS	Debug programs	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. Grant this right only to developers on development computers.

Deny access to this computer from the network (Windows 2000/XP/ Server 2003)

This security check reports accounts that are denied access to a computer from the network. Because this right takes precedence over the Access this computer from the network right, you can use it to deny access to subsets of security groups that have access through the Access right.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
DENY_ACCESS_ FROM_NETWORK	Deny access to this computer from the network	C	0

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from reported users to whom you want to grant the Access this computer from the network right. Until you revoke the Deny right, the Access right does not take effect.

Deny logon as a batch job (Windows 2000/XP/Server 2003)

This security check reports accounts that are denied the ability to log on to the network using a batch-queue facility. Because this right takes precedence over the Log on as a batch job right, you can use it to deny access to subsets of security groups that have access through the Log on right.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
DENY_LOGON_ BATCH	Deny logon as a batch job	C	0

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from reported users to whom you want to grant the Log on as a batch job right. Until you revoke the Deny right, the Log on right does not take effect.

Deny logon as a service (Windows 2000/XP/Server 2003)

This security check reports accounts that are denied the ability to log on to the system as a service. Because this right takes precedence over the Log on as a service right, you can use it to deny access to subsets of security groups that have access through the Log on right.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message	Title	Type	Class
DENY_LOGON_ SERVICE	Deny logon as a service	C	0

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from reported users to whom you want to grant the Log on as a service job right. Until you revoke the Deny right, the Log on right does not take effect.

Deny logon locally (Windows 2000/XP/Server 2003)

This security check reports accounts that are denied the ability to log on to the system locally at the computer keyboard. Because this right takes precedence over the Log on locally right, you can use it to deny access for subsets of security groups that have access through the Log on right.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
DENY_LOGON_ LOCALLY	Deny logon locally	C	0

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from reported users to whom you want to grant the Log on locally right. Until you revoke the Deny right, the Log on right does not take effect.

Deny logon through Terminal Service (Windows XP/Server 2003)

This check reports accounts that cannot log on through Terminal Services. Because this right takes precedence over Allow logon through Terminal Services, you can use it to deny access to subsets of groups that have access through the Allow right.

Use the name list to include or exclude users or security groups that are not included or excluded by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
DENY_LOGON_TERMINAL_SERVICES	Deny logon through Terminal Services	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from reported users to whom you want to grant the Log on through Terminal Services right. Until you revoke the Deny right, the Log on right does not take effect.

Enable computer and user accounts to be trusted for delegation (Windows 2000/Server 2003)

This security check for domain controllers reports accounts with rights to change the Trusted for delegation setting on a user or computer object in the Active Directory.

Note: There is no reason to run this check on a non-domain controller computer. If you do run this check on a non-domain controller computer, ignore anything Symantec ESM reports.

Delegation is used by multi-tier client/server applications. An account with this user right may be able to conduct sophisticated attacks to gain access to network resources.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
ENABLE_TRUSTED_ DELEGATION	Enable computer and user accounts to be trusted for delegation	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. This right should be granted only to users and security groups that require it for normal business functions.

Force shutdown from a remote system

This security check reports accounts with rights to shut down a computer that is running Windows from a remote location on the network.

This standard right is given by default to Administrators on workstations and servers and to Power Users on workstations.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
FORCE_REMOTE_ SHUTDOWN	Force shutdown from a remote system	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. The right should not be granted to any user.

Generate security audits

This security check reports accounts with rights to generate entries in the security log.

By default, this advanced right is not given to users. Users with this right can write enough entries to fill up the security audit log and, depending on other security settings, either halt the system or overwrite critical log entries.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
SECURITY	Generate security audits	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users.

Increase quotas (Windows NT/2000/Server 2003)

This security check reports accounts with rights to increase quotas. Processes that run under accounts with this user right can increase the processor quota of other processes. Abuse of this right can aid a denial-of-service attack.

By default, this advanced right is granted only to the Administrators security group.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
INCREASE_QUOTAS	Increase quotas	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. It should be granted only to members of the Administrators security group.

Increase scheduling priority

This security check reports accounts with rights to increase scheduling priority. Users with this user right can increase the execution priority of processes. Setting the priority high on some processes can deny system time to other processes, causing a denial of service.

By default, this advanced right is granted only to members of the Administrators group on workstations and servers and to Power Users on workstations.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
INCREASE_PRIORITY	Increase scheduling priority	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke this right from users who are not members of the Administrators and Power Users security groups.

Load and unload device drivers

This security check reports accounts with rights to load and unload Plug and Play device drivers.

Memory resident device drivers have no security restrictions on computers running Windows operating systems. Intruders with this right can load trojan horse device drivers into memory to exploit the system.

By default, this advanced right is given only to members of the Administrators security group.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
LOAD_DRIVERS	Load and unload device drivers	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users.

Lock pages in memory (Windows NT)

This security check reports accounts that can lock pages in memory (usually restricted in User Rights Assignments).

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
LOCK_PAGES	Lock pages in memory	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Do one of the following:
  - If the user is authorized to have this right, add the user to the check's name list.
  - If the user is not authorized to have this right, use the Correct feature in the console grid to revoke it.

Log on as a batch job

This security check reports accounts with rights to log on to a system using a batch-queue facility.

By default, this advanced right is given only to members of the Administrators security group.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
LOGON_BATCH	Log on as a batch job	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users.

Log on as a service

This security check reports accounts with rights to log on to the network as a service.

You can configure users to run under an account only if that account has this advanced user right. The Local System account always has this right, but this right is not given to any users by default.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
LOGON_SERVICE	Log on as a service	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. Normally it should not be granted to any user.

Log on locally

This security check reports accounts that have the right to log on to a system locally from the keyboard. Users do not usually need to log on locally to domain controllers.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
LOGON_LOCALLY	Log on locally	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct function in the console grid to revoke this right for unauthorized users.

Manage auditing and security log

This security check reports accounts with rights to configure auditing on Active Directory objects, files, registry keys, and other resources. These accounts can also view and clear the security log.

By default, this standard right is given only to members of the Administrators security group. Users with this right can attack the system, then delete the security log to cover up their activities.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
MANAGE_LOG	Manage auditing and security logs	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct function in the console grid to revoke this right for unauthorized users. This right should be granted only to a limited security group of internal auditors.

Modify firmware environment values

This security check reports accounts with rights to modify system environment variables.

By default, this advanced right is given only to the members of the Administrators security group.

System environment variables determine which executable runs when a user calls a specific file. A user with this right can change the system path to point to a trojan horse program instead of the correct executable. If the trojan horse program calls the original executable, an administrator who is running the executable would not detect the execution of the trojan horse program.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
MODIFY_FIRMWARE_VALUES	Modify firmware environment values	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct function in the console grid to revoke this right from unauthorized users. The right should be granted only to members of the Administrators security group.

Perform volume maintenance tasks (Windows XP)

This check reports accounts with rights to perform volume maintenance tasks.

You can use the check name lists to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
PERFORM_VOLUME_MAINTENANCE_TASK	Perform volume maintenance tasks	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. This right should be granted only to members of the Administrators security group.

Profile single process

This security check reports accounts that have the right to monitor the performance of a single process.

By default, this advanced right is given to members of the Administrators security group on workstations and servers and to Power Users on workstations. A user with this right can monitor the performance of non-system processes.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
PROFILE_PROCESS	Profile single process	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct function in the console grid to revoke this right for unauthorized users. This right should be granted only to members of the Administrators and Power Users security groups.

Profile system performance

This security check reports accounts with rights to profile system performance.

By default, this advanced right is given only to members of the Administrators security group.

With this user right, a user can:

- Monitor the performance of system processes.
- Use the Windows monitor tools to sample the performance of the network that is running Windows.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
PROFILE_SYSTEM	Profile system performance	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- ◆ Use the Correct function in the console grid to revoke this right for unauthorized users. This right should be only granted to members of the Administrators security group.

Remove computer from docking station (Windows 2000/XP/Server 2003)

This security check reports accounts with rights to undock a portable computer.

The check returns the following message:

Message name	Title	Type	Class
UNDOCK_ COMPUTER	Remove computer from docking station	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke this right from unauthorized users. Do not grant the right to any users or security groups that do not require it for normal business functions.

Replace a process level token

This security check reports accounts with rights to replace a process level token.

By default, this advanced right is not given to users.

A process running under an account with this user right can replace the access token of a child process. Users with this right can seriously compromise the security of the system. Windows provides controls to manage this process.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
REPLACE_TOKEN	Replace a process level token	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct function in the console grid to revoke this right for unauthorized users. This right should not be granted to any user.

Restore files and directories

This security check reports accounts with rights to restore files and directories.

By default, this advanced right is given to the Administrators and Backup Operators security groups. Users with this right can overwrite the contents of critical files or directories and change the owner of any file on the system.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
RESTORE	Restore files and folders	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke the right from unauthorized users. Grant the right only to backup operators and members of the Administrators security group.

Shut down the system

This security check reports accounts with rights to shut down the network.

By default, this standard right is given to the Administrators, Backup Operators, Everyone, Power Users, and Users security groups. Users with this right can shut down the system.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
SHUTDOWN	Shut down the system	C	1

For steps to demonstrate the check, see “To demonstrate user rights checks” on page 69.

To protect your computers

- Use the Correct feature to revoke the right from unauthorized users. Grant the right only to backup operators and members of the Administrators security group.

Synchronize directory service data (Windows 2000/Server 2003)

This security check for domain controllers reports domain accounts with rights to synchronize directory service data.

Note: If you run this check on a non-domain controller computer, ignore anything Symantec ESM reports.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
SYNC_DIRECTORY_ SERVICE	Synchronize directory service data	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke the right from unauthorized users. It should be granted only to members of the domain Administrators security group.

Take ownership of files or other objects

This security check reports accounts with rights to take ownership of Active Directory objects, files, registry keys, printers, or other securable objects on the system.

By default, this standard right is given only to the Administrators security group. Users with this right can seriously compromise the security of sensitive information and the operation of critical processes. The right does not include the ability to return objects to their original owners.

Windows can audit this action in the security log.

You can use the name lists in the check to exclude or include users or security groups that are not already excluded or included by the Users to check option.

The check returns the following message:

Message name	Title	Type	Class
TAKE_OWNERSHIP	Take ownership of files or other objects	C	1

For steps to demonstrate the check, see "To demonstrate user rights checks" on page 69.

To protect your computers

- Use the Correct feature to revoke the right from unauthorized users. It should be granted only to members of the Administrators security group.

Create global objects (Windows 2000/XP/Server 2003)

This security check reports users and security groups that have the right to create global objects in a terminal services session.

The check returns the following message:

Message name	Title	Type	Class
SM_CREATE_GLOBAL_OBJECT	Create global objects	C	1

Impersonate a client for authentication (Windows 2000/XP/Server 2003)

This security check reports users and security groups that have the right to impersonate other accounts.

The check returns the following message:

Message name	Title	Type	Class
IMPERSONATE_A_CLIENT	Impersonate a client for authentication	C	1

Active Directory (Windows 2000/Server 2003)

The Active Directory module for Windows 2000 reports group policy objects (GPOs) that apply to users, groups, and computers in the Active Directory Service (ADS). GPOs are active directory objects that contain group policies such as the Windows security policy. GPO settings can be applied to sites, domains, and organizational units.

The module is not included in any of the default policies that ship with Symantec ESM, but it is available when you edit a policy. See “Creating and editing your own policies” on page 30.

Computers with applied GPOs (Windows 2000/Server 2003)

This security check reports group policy objects (GPOs) that apply to the examined computer. Applied GPOs can be inherited from sites, domains, and organizational units.

The check returns the following message:

Message name	Title	Class
COMPUTER_GPOS	Computer GPOs	2

To protect your computers

- Do one of the following:
  - Add computers and users to GPOs that they are authorized for.
  - Remove computers and users from GPOs that they are not authorized for.

Computers without applied GPOs (Windows 2000/Server 2003)

This security check reports computers that do not have group policy objects (GPOs) applied to them through sites, domains, or organizational units. Default GPOs that are applied to the computer are not reported.

The check returns the following message:

Message name	Title	Class
NO_LOCAL_HOST_GPO	Computers without applied GPOs	2

To protect your computers

- Ensure that your security policy is enforced for the reported computers and users.

Users with applied GPOs (Windows 2000/Server 2003)

This security check for domain controllers reports all users with applied group policy objects (GPOs) in an ADS domain.

The check returns the following message:

Message name	Title	Class
USER_GPO_LIST	User GPOs	2

To protect your computers

- Ensure that your security policy is enforced for the reported users.

Users without applied GPOs (Windows 2000/Server 2003)

This security check for domain controllers reports all users in an ADS domain that do not have group policy objects (GPOs) applied to them.

The check returns the following message:

Message name	Title	Class
NO_USER_GPO	User without applied GPOs	2

To protect your computers

- Ensure that your security policy is enforced for the reported users.

Security groups with applied GPOs (Windows 2000/Server 2003)

This security check for domain controllers reports all security groups with applied group policy objects (GPOs) in an ADS domain.

The check returns the following message:

Message name	Title	Class
GROUP_GPO_LIST	Security group GPOs	2

To protect your computers

- Ensure that your security policy is enforced for the reported group.

Security groups without applied GPOs (Windows 2000/Server 2003)

This check reports all security groups in an ADS domain that do not have group policy objects (GPOs) applied to them. The check is intended to run only on domain controllers to produce results for specific domains.

The check returns the following message:

Message name	Title	Class
GROUP_WITHOUT_APPLIED_GPOS	Security group without applied GPOs	2

To protect your computers

- Ensure that your security policy is enforced for the reported group.

Backup Integrity

The Backup Integrity module reports files and folders on local drives that have not been backed up since they were last changed. Backups prevent data loss in the event of a disk or system failure.

Backups needed

This security check reports local drives and the relative number of files on each that have not been backed up since the last snapshot update. It also reports the names of files that have not been backed up since the last snapshot update.

Use the check name list to exclude drives that are never backed up.

The check reports file names up to the number specified in the Max files shown field. The default value is 25. A value of 0 reports no files. A value of -1 reports all files that have not been backed up since the last snapshot update. Due to space limitations in the console grid, the -1 value is not recommended.

Note: To determine the maximum number of files that the check can report, subtract the number of drives on the system from the number of report lines available in the console grid.

Disk or system failures can cause a loss of critical data if you fail to back up important files.

The check returns the following messages:

Message name	Title	Class
A_FEW_FILES	A few files not backed up	1
A_LOT_OF_FILES	A lot of files not backed up	1
FILE_NOT_BACKUP	File not backed up	0
MORE_FILES	Many files not backed up	1
THE_WHOLE_DRIVE	No backups performed on this drive	4

To demonstrate the check

1. In a demo policy, disable all checks in the Backup Integrity module except Backups needed.
2. Select a test directory directly under root on a drive that is not backed up.
3. Click the archive check box of a test file in the test directory.

4 Edit the name list in the Backups needed check to exclude all drives on the host system except the drive containing the test directory.

5 Edit the name list in the module's Folders excluded option to exclude all directories on the drive except the test directory.

6 Run the demo policy on the agent.

7 Verify that File not backed up is reported.

To protect your computers

◆ Back up files often enough to minimize data loss.

Folders excluded

Use this option to specify directories that you want to exclude from the check. By default, the check examines all directories on the system.

Add directories to the name list only if they are directly under root. For example, C:\WINNT is a valid entry but C:\WINNT\SYSTEM32 is not. Also, C:\WINNT\ is not valid because it ends with a back slash.

Discovery

The Discovery module reports computers that could run Symantec ESM or Symantec Intruder Alert but are not running them. The Discovery module is in the Queries policy.

Targets

Use this option to specify target IP addresses to be scanned. Each target address has four parts with periods separating the parts, and can represent one or more IP addresses. Each part consists of a number between 1 and 254, a range of numbers, or a wildcard character (* or ?). A range of numbers is specified as n-m where n is the lower limit and m is the upper limit. If the lower limit is not specified (for example, -127), 1 is used. If the upper limit is not specified (for example, 17-), 254 is used.

An * represents the range of numbers 1-254. A ? represents the matching part of the agent's IP address. These numbers, ranges of numbers, and wildcard characters can be used in combinations to specify complex sets of IP addresses.

For example, if the range 172.17.10-20.* is specified, the addresses 172.17.10.1, 172.17.10.2, ..., 172.17.10.254, 172.17.11.1, ..., 172.17.11.254, ..., 172.17.20.254 are scanned.

The range of IP addresses an agent can scan is limited based on the Class of the agent's IP address. The first number in an agent's IP address determines the address class. If the first number is between 1 and 126, the agent's address is Class A. If it is between 128 and 191, the agent's address is Class B. If it is between 192 and 223 the agent's address is Class C.

For example, if the agent's address is 10.168.17.7 (a class A address,) it can scan any IP address in the same class A range, or any address with a first part of 10 (10.*.*.*). An agent with an IP address of 192.168.17.7 (a class C address,) can only scan the addresses 192.168.17.1-192.168.17.254.

Symantec ESM device status

This check examines specified TCP ports on devices that are targeted in the Targets option, and reports devices that are not running Symantec ESM.

To report computers that could run Symantec ESM but are not (candidates), enable the Profile candidate devices option.

To report computers that are running Symantec ESM, enable the Report if found option.

This security check reports Symantec ESM candidate systems that are in the same licensed address class as the module running the check when Check known TCP ports on IP addresses is enabled.

The check also reports systems where Symantec ESM is installed and running when Report if found is enabled.

Use the check’s name list to specify TCP port numbers that you want to be examined and are not already specified in the Targets option.

- Change the port number in the name list if the agent runs the current version of Symantec ESM but does not use the current, default port number.
- If the agent is running previous versions of Symantec ESM, they may use different port numbers. To examine previous installations, add their port numbers to the name list. See Appendix B, “ESM communications,” in the *ESM Installation Guide* for port numbers.

The check returns the following messages:

Message name	Title	Class
ESM_CANDIDATE	ESM candidate	2
ESM_FOUND	ESM found	0
INV_ADDRQUAL	Invalid address qualifier	2
NOT_ESM_ CANDIDATE	Non-ESM candidate	0
TIMED_OUT	Timed out while profiling	0

If Non-ESM candidate is reported, Symantec ESM was not found at the address or on the host, and the responding hardware does not appear to be a candidate for a Symantec ESM installation.

Common measures employed to secure computers can prevent the module from identifying remote operating systems. The more secure a remote computer, the less likely the module will be able to identify the operating system. If it cannot be identified, Symantec ESM reports this message.

If Invalid address qualifier is reported, correct the addresses specified in the name list and/or Targets option.

To demonstrate the check

1. In a demo policy, disable all checks and options of the Discovery module except:
   - Symantec ESM device status
   - Targets
   - Report if found
2. Run the demo policy on the agent.
3. Verify that Symantec ESM candidate or Symantec ESM found is reported.

To protect your computers

- Install Symantec ESM on all reported candidates.

Symantec Intruder Alert device status

This check examines the specified TCP ports on devices that are specified in the Targets option and reports devices that are not running Symantec Intruder Alert.

To report computers that could run Symantec Intruder Alert but are not (candidates), enable the Profile candidate devices option.

To report computers that are running Symantec Intruder Alert, enable the Report if found option.

Use the check's name list to specify TCP ports that you want to be examined and are not already specified in the Targets option.

An agent's Symantec Intruder Alert TCP port number is displayed as the agent's Service Setting in the Symantec Intruder Alert Administrator.

The check reports the following messages:

Message name	Title	Class
ITA_CANDIDATE	ITA candidate	2
ITA_FOUND	ITA found	0
INV_ADDRQUAL	Invalid address qualifier	2
NOT_ITA_CANDIDATE	Non-ITA candidate	0
TIMED_OUT	Timed out while profiling	0

If Non-ITA candidate is reported, Symantec Intruder Alert was not found at the address or on the host, and the responding hardware does not appear to be a candidate for a Symantec Intruder Alert installation.

Common measures employed to secure computers can prevent the module from identifying remote operating systems. The more secure a remote computer, the less likely the module will be able to identify the operating system. If it cannot be identified, Symantec ESM reports this message.

If Invalid address qualifier is reported, correct the addresses specified in the name list and/or Targets option, then rerun the module.

To demonstrate the check

1. In a demo policy, disable all checks and options in the Discovery module except:
   - Symantec Intruder Alert device status
   - Targets
   - Report if found
2. Run the demo policy on the agent.
3. Verify that ITA candidate or ITA found is reported.

To protect your computers

◆ Install a Symantec Intruder Alert or the new Symantec Host IDS on all reported candidates.

Report if found

When this option is enabled, the module reports computers that are running Symantec ESM or Intruder Alert.

Profile candidate devices

When this option is enabled Symantec ESM and Symantec Intruder Alert candidates are reported for Symantec ESM and Intruder Alert device status checks.

When the option is disabled, only computers currently running these products are reported. All devices that are not running them are reported as non-candidates.

This is a time consuming option. Though it does not tax CPU usage, profiling can take several minutes per IP address.

Profiling examines the following ports to determine the type of network device: tcpmux 1, echo 7, discard 9, systat 11, daytime 13, netstat 15, quote 17, ttytst 19, ftp 21, telnet 23, smtp 25, time 37, domain 53, finger 79, http 80, pop-2 109, pop-3 110, rpcbind 111, loc-srv 135, netbios-ssn 139, exec 512, login 513, shell 514, printer 515, uucp 540, and x-server 6000.

Profile timeout

This option specifies the maximum number of seconds that a module spends profiling a candidate system before aborting and going to the next address.

The timeout value cannot be less than 15 seconds or greater than 900 seconds (15 minutes).

This timeout value does not override the computer default timeout value. When the value that is set in this option is less than the computer value, the overall time required to complete a module run may be reduced.

Scan non-responding addresses

When this option is enabled, module checks scan all IP addresses that are specified in the Targets option, including those that do not respond to a ping. Enabling this option greatly increases the time required to complete the scan.

Service	Port	Service	Port	Service	Port
tcpmux	1	echo	7	discard	9
systat	11	daytime	13	netstat	15
quote	17	ttytst	19	ftp	21
telnet	23	smtp	25	time	37
domain	53	finger	79	http	80
pop-2	109	pop-3	110	rpcbind	111
loc-srv	135	netbios-ssn	139	exec	512
login	513	shell	514	printer	515
uucp	540	x-server	6000		

Note: Enable this option to obtain an accurate report of Symantec ESM or Symantec Intruder Alert candidate systems from the module. Otherwise, computers are reported as non-candidates.

Disk Quota (Windows 2000/XP)

The Disk Quota module reports how disk quota information is tracked and reports a problem if it is not tracked.

Volume quota not supported (Windows 2000/XP)

This security check reports volumes with file systems that do not support quota management.

The system cannot control how much available disk space a user takes on reported volumes. Users that monopolize available space can deny this resource to other users.

The check returns the following message:

Message name	Title	Class
QUOTA_NOT_ SUPPORTED	Volume quota not supported	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume quota not supported.
2. In Windows Explorer, identify a FAT-formatted volume on computer's hard disk.
3. Right-click the FAT-formatted volume, then click **Properties**.
4. Verify that the Quota tab is not displayed.
5. Run the demo policy on the agent computer.
6. Verify that Volume quotas not supported is reported.

To protect your computers

- Do one of the following:
  - Convert volumes on agent systems to NTFS version 5.0 or later.
  - Impose quotas so that all users that access volumes can effectively use the available space.

Volume quota disabled (Windows 2000/XP)

This security check reports volumes that support quota management but have disabled quotas.

The system cannot control how much available disk space a user takes on reported volumes. Users that monopolize available space can deny this resource to other users.

The check returns the following message:

Message name	Title	Class
QUOTA_DISABLED	Volume quotas not enabled	4

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume quota disabled.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Verify that the Enable quota management check box is clear.
5. Run the demo policy on the agent computer.
6. Verify that Volume quotas not enabled is reported.

To protect your computers

- Enable quotas on all volumes that support quota management.
  If you enable but do not enforce quotas, you can monitor usage over time. This can help to determine each user’s actual needs so that appropriate quota limits can be set.

Volume quota not enforced (Windows 2000/XP)

This security check reports volumes that have volume quotas that are enabled but not enforced.

The system cannot control how much of the available space a user takes on these volumes. Users that monopolize available space can deny the resource to other users.

The check returns the following message:

Message name	Title	Class
QUOTA_NOT_ENFORCED	Tracked quotas not enforced	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume quota not supported.
2. In Windows Explorer, right-click the volume, then click **Properties**.
3. Click **Quota**.
4. Run the demo policy on the agent computer.
5. Verify that Tracked quotas not enforced is reported.

To protect your computers

- Enable quotas on all volumes that support quota management. Properly managed quotas let system space be shared by all users.

Volume quota enforced (Windows 2000/XP)

This security check reports volumes where quotas are enabled and enforced.

Properly configured quotas let users store and take ownership of files without disrupting other users on the volume.

The check returns the following message:

Message name	Title	Class
QUOTA_ENFORCED	Volume quotas enforced	0

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume quota enforced.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Verify that the Deny disk space to users exceeding quota limit check box is checked.
5. Run the demo policy on the agent computer.
6. Verify that Volume quotas enforced is reported.

To protect your computers

- Enforce quotas on all volumes that support quota management.

Volume quota exceeds limit (Windows 2000/XP)

This security check reports volumes with quotas that are greater than the specified number of megabytes (MB). The default value is 100 megabytes.

Quota settings should comply with your security policy so that users deny disk space to other users.

The check returns the following message:

Message name	Title	Class
QUOTA_GREATER_THAN_X	Quotas greater than value	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume quota exceeds limit.
2. In the check next to Default Quota Greater than, type **12**.
3. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
4. Click **Quota**.
5. In the Limit disk space field, type **15**.
6. Run the demo policy on the agent computer.
7. Verify that Quotas greater than value is reported.

To protect your computers

- Set quotas on all volumes to no less than 100 megabytes.

Volume warning exceeds limit (Windows 2000/XP)

This security check reports volumes with warning levels that are greater than the specified number of megabytes (MB). The default value is 100 megabytes.

Warning settings should comply with company policy so that users can take corrective actions before running out of disk space.

The check returns the following message:

Message name	Title	Class
WARNING_GREATER_THAN_X	Quota warning level greater than value	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume warning exceeds limit.
2. In the check next to Quota Warning Greater than, type **12**.
3. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
4. Click **Quota**.
5. In the Warning level field, type **15**.
6. Run the demo policy on the agent computer.
7. Verify that Quota warning level greater than value is reported.

To protect your computers

- Set warning levels on all volumes to no less than 100 megabytes.

Volume quota not logged (Windows 2000/XP)

This security check reports volumes that do not log an event when users exceed their quota limits.

If the computer logs these events, you can monitor volume space usage over time to determine each user's actual needs and set appropriate quota limits.

The check returns the following message:

Message name	Title	Class
QUOTA_NOT_LOGGED	Volume quota violations not logged	3

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume quota not logged.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Verify that the Log event when a user exceeds their quota limit check box is clear.
5. Run the demo policy on the agent computer.
6. Verify that Volume quota violations not logged is reported.

To protect your computers

- Configure all volumes to log events when users exceed their quota limits.

Volume warning not logged (Windows 2000/XP)

This security check reports volumes that do not log an event when users exceed their warning levels.

If the computer logs these events, you can monitor volume space usage over time and set appropriate warning levels.

The check returns the following message:

Message name	Title	Class
WARNING_NOT_LOGGED	Volume warnings not logged	3

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Volume Warning Not Logged.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Verify that the Log event when a user exceeds their warning level check box is clear.
5. Run the demo policy on the agent computer.
6. Verify that Volume warnings not logged is reported.

To protect your computers

◆ Configure all volumes to log events when users exceed their warning levels.

User quota not enforced (Windows 2000/XP)

This security check reports users that do not have quota limits on volumes.

The system cannot control how much space these users take. They can monopolize available space and deny disk space to other users.

The check returns the following message:

Message name	Title	Class
USER_NO_QUOTA	User has no quota limit	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except User quota not enforced.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Click **Quota**
5. Select a user.
6. On the Menu bar, click **Quota** > **Properties** > **Do not limit disk usage**.
7. Run the demo policy on the agent computer.
8. Verify that User has no quota limit is reported.

To protect your computers

◆ Enforce quotas on all users that are not members of the Administrators security group.

User exceeds quota (Windows 2000/XP)

This security check reports users that exceed their quota limits on a volume.

Users that monopolize available space deny resources to other users.

The check returns the following message:

Message name	Title	Class
USER_OVER_QUOTA_ LIMIT	Quota level exceeded	4

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except User exceeds quota.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Click **Quota Entries**.
5. Select a user that has an Amount Used that exceeds the quota limit and is not a member of the Administrators security group.
6. Run the demo policy on the agent computer.
7. Verify that Quota level exceeded is reported.

To protect your computers

- Enforce quotas on all users that are not members of the Administrators security group.

User exceeds warning (Windows 2000/XP)

This security check reports users that exceed their quota warning levels on a volume. Warning levels alert users to take corrective actions before running out of disk space.

The check returns the following message:

Message name	Title	Class
USER_OVER_WARNING_ LIMIT	Quota warning level exceeded	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except User exceeds warning.
2. In Windows Explorer, right-click an NTFS volume, then click **Properties**.
3. Click **Quota**.
4. Click **Quota Entries**.
5. Select a user that has an Amount Used that exceeds the warning level and is not a member of the Administrators security group.
6. Run the demo policy on the agent computer.
7. Verify that Quota warning level exceeded is reported.

To protect your computers

- Set warning levels on all volumes to comply with your security policy.

Encrypted File System (Windows 2000/XP)

The Encrypted File System module checks to see if the Encrypted File System (EFS) is supported and being used. It also reports different aspects of the EFS configuration.

EFS not supported (Windows 2000/XP)

This security check reports volumes with file systems that do not support the Encrypted File System (EFS).

The system cannot encrypt files on these volumes. If intruders can access the volumes, they can open the files that are contained in the volumes.

The check returns the following message:

Message name	Title	Class
EFS_NOT_SUPPORTED	EFS not supported	2

To demonstrate the check

1. In a demo policy, disable all checks in the Encrypted File System module except EFS not supported.
2. In Windows Explorer, identify a volume on the agent computer’s hard disk that is FAT-formatted.
3. Click the FAT-formatted volume.
4. Right-click a folder or file, then click **Properties**.
5. Click **General** > **Advanced**.
6. Verify that the Encrypt contents to secure data check box is not displayed.
7. Run the demo policy on the agent computer.
8. Verify that EFS not supported is reported.

To protect your computers

- Do one of the following:
  - Convert volumes on agent systems to NTFS version 5.0 or later.
  - Encrypt critical folders and files.

Percentage of encrypted files (Windows 2000/XP)

This security check reports the percentage of encrypted files on each volume.

Intruders with unauthorized access can open critical but unencrypted files on volumes.

The check returns the following message:

Message name	Title	Class
EFS_PERCENTAGE	EFS percentage	0

To demonstrate the check

1. In a demo policy, disable all checks in the Encrypted File System module except Percentage of encrypted files.
2. In Windows Explorer, right-click an NTFS volume, then click a test folder.
3. Click **Properties** > **General** > **Advanced**.
4. Verify that the Encrypt contents to secure data check box is checked.
5. Run the demo policy on the agent computer.
6. Verify that EFS percentage is reported.

To protect your computers

- Encrypt critical folders and files on NTFS volumes.

Files can be decrypted by others (Windows 2000/XP)

This security check reports files that can be decrypted by users other than the file owner.

Each encrypted file contains a list of users that can decrypt the file. Encryption should prevent unauthorized access to critical information until the file can be returned to the correct owner.

Use the name lists to exclude users and security groups from the check.

Authorized file ownership changes should never involve encrypted files. New owners cannot open files that were encrypted by previous owners.

If a user other than the owner can decrypt a file, an unauthorized change in file ownership may have occurred.

The check returns the following message:

Message name	Title	Class
EFS_DECRYPTED_BY_OTHERS	File can be decrypted by others	2

To demonstrate the check

1. In a demo policy, disable all checks in the Disk Quota module except Files can be decrypted by others.
2. In Windows Explorer, right-click an NTFS volume, then click a test folder.
3. Click **Properties** > **General** > **Advanced**.
4. Verify that the Encrypt contents to secure data check box is checked.
5. Change the owner of the encrypted file to another user.
6. Run the demo policy on the agent computer.
7. Verify that File can be decrypted by others is reported.

To protect your computers

- Do one of the following:
  - Decrypt files before changing ownership.
  - For unauthorized changes, restore files to their correct owners.

File recovery agents not authorized (Windows 2000/XP)

This security check reports encrypted files that have recovery agent thumb prints or names that do not match entries in the name lists.

Specify the recovery agent thumb prints or names for the check by adding them to the name lists. The check cannot detect any recovery agent errors if the name lists are blank.

The check returns the following messages:

Message name	Title	Class
EFS_RECOVERY_AGENTS_THUMBPRINT	Recovery agent thumb print not authorized	2
EFS_OTHER_RECOVERY_AGENTS	Recovery agent name not authorized	2

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except File recovery agents not authorized.
2. Add recovery agent thumb prints or names to the name lists in the check.
3. In Windows Explorer, right-click an NTFS volume, then click a test folder.
4. Click **Properties** > **General** > **Advanced**.
5. Verify that the Encrypt contents to secure data check box is checked.
6. Verify that Recovery agent thumb print not authorized or Recovery agent name not authorized is reported.

To protect your computers

- Encrypt the reported files using valid recovery agents.

File Attributes

Security checks in the File Attributes module compare current settings with File template records and report changes in file ownership, size, creation time, and modification. The module also reports changes in access control lists (ACLs), results of checksum checks, and folders for which the Everyone group has full control permissions.

Some messages report messages that you can use to update template or snapshot files to match current agent settings. See "Updating template and snapshot files in messages" on page 42.

Other checks report messages that you can use to reverse agent settings or disable user accounts. See "Correcting agents in messages" on page 42.

Updateable and correctable messages are identified as TU, SU, or C types in the descriptions of checks that use them.

Common File Attributes messages

When you run a policy that contains the File Attributes module, the module compares current file attributes to records in File templates before it runs enabled security checks.

The following messages may be reported before any security checks are run:

Message name	Title	Class
ADDITIONAL_SACL_ENTRY	Additional SACL entry	1

Message name	Title	Class
DIFFERENT_SACL_ENTRY	Different SACL entry	1
FILE_LOCKED	Locked file	0
FILE_MISSING	No template files specified	4
FILE_NOT_FOUND	File or folder not found	0
FORBID	Forbidden file exists	4
FORBIDWC	Forbidden wild card file exists	4
MISSING_SACL_ENTRY	Missing SACL entry	1
NOEXIST	Mandatory file does not exist	4
NOEXISTWC	Mandatory wild card entry	4

Note: The module examines the File Keywords template for file path names that are identified by variable keywords are enclosed in percent (%) signs in the File template. When the module does not find a match, it handles the path name as it would if it did not contain a keyword. If the file is mandatory and the module cannot match the file name, it reports Mandatory file does not exist.

File templates are enabled in the Template file list option.

Template file list

Use this option to enable or disable the File template files that are used by File Attributes security checks.

The template types are:

- Windows Server 2003 .s52
- Windows XP Professional .w51
- Windows 2000 Professional .w50
- Windows 2000 Server .s50
- Windows NT 4.0 Servers .s40
- Windows NT 4.0 Workstations .w40

Editing the File template

Do not edit the File template that is installed with Symantec ESM. Instead, add your own template.

To add a new File template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Create New Template dialog box, click the type of template that you want to add. The template type determines the file extension of the new template file.
3. Type a new template name of no more than eight characters.
4. Do one of the following:
   - Load a single file with its current attributes. See "To load attributes of a single file" on page 115.
   - Load all files in a folder with their current attributes. See "To load attributes of all files in a folder" on page 115.
   - Manually add new file records. See "To manually load attributes of a file" on page 116.
5. Press **Enter** or click **OK**.

To load attributes of a single file

1. In the Template Editor, click **Add File**.
2. In the Add Items to Template dialog box, click the Agent name field, then select the agent where the file is located.
3. In the Item name text box, type the path of the file on the agent.
   Use the format <volume>:\<folder>\<subfolder>\<file>. Do not start the path name with double or single back slashes or forward slashes.
4. Press **Enter**.

To load attributes of all files in a folder

1. In the Template Editor, click **Add Directory**.
2. Click the Agent name field, then select the agent that has the folder.
3. In the Item to add text box, type the folder path for the module.
4. Select the option that describes the level of subordinate folders and files that you want to load from the Items to include group. Each subordinate level includes the files that are located within that level.
5. Click **OK**.

To manually load attributes of a file

1 In the Template Editor, click **Add Row**.

New rows are added to the bottom of the table. You may need to scroll to the bottom of the table to see it.

2 In the Folder/File Name field of the new row, replace <NEW> with the path and name of the folder or file that you want to track.

Do not start the file or folder path name with double or single back slashes or forward slashes.

Valid folder and file path names can include variable keywords that represent data in Windows registry values. Most keywords must be defined in the File Keywords template before they are used in the File templates. See "Editing the File Keywords template" on page 122.

3 In the Owner field of the new row, replace <NEW> with the name of the file owner.

4 In the Attributes field, replace <NEW> with values for the read/write, hidden, and system file attributes for Windows 2000 Server (.s50) and Professional (.w50), Windows XP (.w51), and Server 2003 (.s52):

Table 5-1 Windows 2000/XP/Server 2003

Position	Character	Attribute
1	R or r	Read
2	W, w, O, or o	Write / Only
3	[space]	
4	- [hyphen], H, or h	Normal / Hidden
5	[space]	
6 and 7	-- [two hyphens], SY, or sy	Required system file

For example, Rw - - -- is for a file with read/write attributes that is neither hidden, nor is it a required system file.

The values for Windows NT (.s40 and .w50) are:

Table 5-2 Windows NT

Position	Character	Attribute
1	R or r	Read
2	W, w, O, or o	Write / Only
3	[space]	
4	- [hyphen], A, or a -	Archive [for backwards compatability only]
5	-, H, or h -	Normal / Hidden
6	[space]	
7 and 8	-- [two hyphens], SY, or sy	Required system file

5 Check the Create Time, Modify Time, or File Size check boxes to track the date and time that a file was created, when it was last changed, and what its current file size should be. Current settings are stored in a snapshot file the first time the module is run.

6 Click the Signature field in the row that you are editing, then select one of the following:

- **None** No signature
- **CRC** 16-bit signature
- **MD5** 128-bit signature
- **CRC+MD5** Combined CRC and MD5

Note: Signature values are stored in the siffile.dat snapshot file.

7 Click the Required field in the row that you are editing, then select one of the following:

- **Optional** File existence is optional.
- **Mandatory** File must exist.
- **Forbidden** File must not exist.

8 Check **Enable ACL Checking** to track changes in access control lists.

9 Add entries to the Permissions ACL sublist.

10 Add entries to the Auditing ACL sublist.

11 In the Comments field, replace <NEW> with any additional text that you want to display with File Attributes messages for the file or folder.

Editing a Permissions ACL sublist

The File Attributes module uses information in the Permissions ACL sublist to verify file and folder permissions on volumes with NTFS partitions. Standard permissions consist of a set of specific permissions. For example, the standard Read permission includes the specific permissions Read Permissions, List Folder/Read Data, Read Extended Attributes, and Read Attributes.

To set standard file and folder permissions

1. In Windows Explorer, right-click a folder or file, then click **Properties**.
2. Click **Security.**
3. Specify settings, then click **OK**.

To set specific permissions

1. Follow steps 1 and 2 above, then click **Advanced**.
2. Click **Permissions** > **View/Edit**.

If you run a policy with a Permissions ACL sublist that has no entries, the File Attributes module reports any Permissions ACLs that it finds as additional Permissions ACL entries.

To add a row to the Permissions ACL sublist

1. In the Template Editor, click the **Permissions ACL** field in the row that you are editing.
2. Click **Add Row**.
3. In the User/Group field, replace <NEW> with the name of the user or group.
4. In the Object Permissions field, replace <NEW> with the permissions that you want the user or security group to have on the file or folder. Every permission is assigned a letter to represent it:

Change Permissions	P
Create Directories/Append Data	A
Create Files/Write Data	W
Delete	D
Delete Subfolders and Files	U
List Directory/Read Data	R
Read Attributes	Q

Read Extended Attributes	N
Read Permissions	E
Take Ownership	O
Traverse Directory/Execute File	X
Write Attributes	T
Write Extended Attributes	B

To specify multiple permissions, type the corresponding letters in any order without spaces or punctuation. For example, to specify Read Attributes (Q) and Write Attributes (T), you would type QT.
Some common permission combinations can be written in the following ways:

Full Control	DEPORWANBXUQT
Modify	DERWANBXQT
Read & Execute	ERNXQ
List Folder Contents	ERNXQ
Read	ERNQ
Write	WABT
(None)	[Blank]

You cannot combine different methods of writing permissions. For example, to specify the standard Read permission plus the Write Attributes permission, type ERNQT, not ReadT.

5. Click **Apply**.
   To add another row, repeat steps 2–5.
6. Click **Close**.

Editing an Auditing ACL sublist

The File Attributes module uses entries in the Auditing ACL sublist to monitor file/folder access events (successes and failures) by users and security groups on volumes with NTFS partitions.

Auditing ACLs are written as SACLs.

If an Auditing ACL sublist has no entries, the module reports any SACLs that it finds as additional SACL entries.

To add a row to an Auditing ACL sublist

1 In the Template Editor, click the **Auditing ACL** field in the row that you are editing.

2 Click **Add Row**.

3 In the User/Group field, replace <NEW> with the name of the user or security group.

4 In the Success field, replace <NEW> with the events that the computer should audit if the user is successful.

Valid values for Success field

Full Control (W2K, XP only)

All (NT only)

Modify (W2K, XP only)

Read and Execute (W2K, XP only)

List folder contents (W2K, XP only)

Read (W2K, XP only)

Write (W2K, XP only)

None (W2K, XP only)

RrWwXxDdPpOoQqNnAaTtBbUuEeSs
See the table in step 4 of "To add a row to an ACL sublist" on page 225.

5 In the Failure field, replace <NEW> with the events that the computer should audit if the user is not successful.

Valid values for Failure field

Full Control (W2K, XP only)

All (NT only)

Modify (W2K, XP only)

Read and Execute (W2K, XP only)

List folder contents (W2K, XP only)

Read (W2K, XP only)

Write (W2K, XP only)

None (W2K, XP only)

RrWwXxDdPpOoQqNnAaTtBbUuEeSs
See the table in step 4 of "To add a row to an ACL sublist" on page 225.

Keywords list

This option lets you enable or disable File Keywords templates that other File Attributes templates use to locate file path names by registry key values.

If you disable the default File Keywords template (windows.fkl), the File Attributes module will not resolve path names that use predefined keywords in the File template.

After you define a keyword in the File Keywords template, you can use it in a file path name in the File template.

Note: You can also use the variable keyword %SystemRoot% in File templates. The File Attributes module finds %SystemRoot% and other predefined Windows keywords in the operating system.

If the module does not find a match for an expected keyword, it handles the path name as it would if it did not contain a keyword. If the file is mandatory and the module cannot match the file name, it reports mandatory file does not exist.

Editing the File Keywords template

File Keywords templates define variable keywords by registry key values. The default windows.fkl template contains keywords for file path names.

To add a new File Keywords template

1. In the enterprise tree, right-click the Templates node, then click **New**.
2. If **File Keywords-all** is not already selected, click it.
3. In the Template file name text box, type a new name of no more than eight characters, without a file name extension. The .fkl extension is added automatically.
4. Press **Enter** or click **OK** to save the template and open the Template Editor.

To add a row to a File Keywords template

1. If the Template Editor is not already open, double-click the name of the template that you want to edit in the Templates branch of the enterprise tree.
2. Click **Add Row**.
3. In the Keyword field, replace <NEW> with the keyword that you want to use to represent the file's registry key value.
   Keywords begin and end with percentage characters (%). For example, %KeywordName%
4. In the Keyword Value field, replace <NEW> with the full path of the Windows registry key value that the keyword will represent.
5. If **Registry** does not appear in the Keyword Type field, click the field, then click **Registry**.
6. Click **Save**.
   To add another row, repeat steps 2–6.
7. Click **Close**.

File ownership

This security check reports files with owners that do not match the owners that are specified in the File template.

Owners have Full Control over files.

The check returns the following messages:

Message name	Title	Type	Class
FILEAT_OWNER_MMAT	Different file ownership	TU / C	1
FILEAT_OWNER_NOT_FOUND	Specified owner not found		1

To demonstrate the check

1. In a demo policy, disable all checks in the File Attributes module except File ownership.
2. In the Template File List option, enable the File template that lists the files that you want to examine. See "Template file list" on page 114.
3. In the Templates branch of the enterprise tree, double-click the name of the enabled template.
4. Do one of the following:
   - To demonstrate Different file ownership, change the owner of a test file in the template to another valid user or group name.
   - To demonstrate Specified owner not found, change the owner of a test file in the template to an invalid user or group name.
5. Run the demo policy and verify that the appropriate message is reported.

To protect your computers

1. Determine if the reported changes in file ownership are authorized.
2. Do the following:

If	Then
The changes are authorized for all systems that use the policy	**Update the File template.** 1 Right-click the Updateable/ field of the console grid, then click **Update Template**. 2 Click **OK**.
The changes are authorized for only some systems that use the policy	**Create a template for the systems where the changes are correct.** 1 Copy the existing template and save it with a new name. 2 In the Template Editor, edit file ownerships for the authorized changes. 3 Copy the policy that uses the original template and save it with a new name. 4 In the new policy, go to the Template File List option of the File Attributes module. 5 Disable the old template and enable the new template. 6 When assessing future file ownership changes, run the new policy on the systems where previously reported changes were authorized.
The changes are not authorized	**Correct the file ownership.** 1 Right-click the Updateable/Correctable field of the console grid, then click **Correct**. 2 Type the user name and password of an account that has the Restore Files and Directories right or the Take Ownership right. 3 Click **OK**.

File attributes

This security check reports files that have Read-only, Hidden, or System attributes that do not match the attributes that are specified in a File template.

File attribute changes can indicate unauthorized activities when they are implemented by someone other than the file owner.

The check returns the following message:

Message name	Title	Type	Class
ATTRIB_MISMATCH	Different file attributes	TU / C	1

To demonstrate the check

1. In a demo policy, disable all checks in the File Attributes module except File attributes.
2. In Windows Explorer, verify that a test file has a Read-only, Hidden, or System attribute. (Right-click the test file, then click **Properties** and confirm that the appropriate check box is checked.)
3. In the Templates branch of the enterprise tree, double-click the enabled template.
4. In the Template Editor, change the Attributes setting of the test file to Rw - - --

   Note: The Archive attribute is not checked by the module.

5. In the Template File List option, enable the File template that lists the files that you want to examine. See “Template file list” on page 114.
6. Run the demo policy and verify that Different file attributes is reported.

To protect your computers

- Do one of the following:
  - For authorized changes, update the template file in the console grid.
  - For unauthorized changes, restore the file from a backup or from the original distribution media.
  - For increased security, run the Changed files (signature) check. See “Changed file (signature)” on page 128.

Changed file (times)

This security check reports files that have creation or modification times that do not match the times in the agent snapshot. File template records determine which files are checked.

Changes can indicate unauthorized activities when implemented by someone other than the file owner.

The check returns the following message:

Message name	Title	Type	Class
SNAPSHOT_MISMATCH	File has changed	SU	1

To demonstrate the check

1. If you have not already done so, run the module to create the agent snapshot file.
2. In the demo policy, disable all checks in the File Attributes module except Changed file (times).
3. In the Template Editor, verify that the Creation Time and Modify Time check boxes are checked for the test file.
4. In the Template File List option, enable the File template that lists the files that you want to examine. See “Template file list” on page 114.
5. Open the file in its associated application. For example, if the test file is a text file, start Notepad.
6. Change the contents of the test file.
7. Run the demo policy and verify that File has changed is reported.

To protect your computers

◆ Do one of the following

- For authorized changes, update the snapshot in the console grid.
- For unauthorized changes, restore the file from a backup or from the original distribution media.
- For increased security, run the Changed file (signature) check. See “Changed file (signature)” on page 128.

Changed file (size)

This security check reports files that have sizes that do not match those in the agent snapshot.

These changes can indicate unauthorized activities when implemented by someone other than the file owner.

The check returns the following message:

Message name	Title	Type	Class
SNAPSHOT_MISMATCH	File has changed	SU	1

To demonstrate the check

1. If you have not already done so, run the module to create the agent snapshot file.
2. In the demo policy, disable all checks in the File Attributes module except Changed file (size).
3. In the Template File List option, enable the File template that lists the files that you want to examine. See "Template file list" on page 114.
4. In the Templates branch of the enterprise tree, double-click the name of the enabled template.
5. In the Template Editor, Ensure that the File Size check box is checked.
6. In the file's related application, change the file contents and save the changes.
7. Run the demo policy and verify that File has changed is reported.

To protect your computers

◆ Do one of the following

- For authorized changes, update the snapshot in the console grid.
- For unauthorized changes, restore the file from a backup or from the original distribution media.
- For increased security, run the Changed file (signature) check. See "Changed file (signature)" on page 128.

Changed file (signature)

This security check reports files that are specified in the File template and that have CRC and/or MD5 signatures that do not match the values of the agent snapshot file.

The check returns the following messages:

Message	Title	Type	Class
SNAPSHOT_MISMATCH	File has changed	SU	1

To demonstrate the check

1. If you have not already done so, run the module to create a snapshot file.
2. In a demo policy, disable all checks in the File Attributes module except Changed file (signature).
3. In the Template Editor, check **Enable ACL Checking** for the test file.
4. In the Template file list option, enable the File template that lists the files that you want to examine. See "Template file list" on page 114.
5. Start the associated application. For example, if the test file is a text file, start Notepad.
6. Change the contents of the test file and save it.
7. Run the demo policy and verify that File has changed is reported.

To protect your computers

- Do one of the following:
  - For authorized changes, update the snapshot in the console grid.
  - For authorized changes, restore the file from a backup or from the original distribution media.

Note: The File Attributes module cannot perform signature checks on the unencrypted contents of Windows 2000 encrypted files. Instead, the module performs signature checks on the raw, encrypted versions of these files.

Consequently, this check can report changes to file signatures even when the contents of the files have not changed. For example, the check reports a signature change for any file that has been encrypted or decrypted or that has had user or file recovery agent changes.

File ACL

This security check reports files with:

- Permissions settings that do not match the template.
- Event audit settings that do not match the auditing sublists in the template.

Note: If you increase the security of folder or file permissions, or increase audited events and want this check to report the change, disable the Do not notify if file permissions are increased in security option.

The check returns the following messages. Messages with an asterisk (*) are correctable in NT systems.

Message name	Title	Class
ADDITIONAL_ENTRY	Additional ACL Entry*	1
ADDITIONAL_SACL_ENTRY	Additional SACL Entry	1
DIFFERENT_ENTRY	Different ACL Entry*	1
DIFFERENT_SACL_ ENTRY	Different SACL Entry	1
MISSING_ENTRY	Missing ACL Entry*	1
MISSING_SACL_ ENTRY	Missing SACL Entry	1
NOACL	File stored on volume that does not support ACLs	1
NOOWNER	Account specified in template does not exist on system	1

To demonstrate the check

1. In a demo policy, disable all checks in the File Attributes module except File ACL.
2. In Windows Explorer, verify that a test file gives Full Control to the Everyone group. (Right-click the test file, then click **Properties** and confirm that the appropriate check box is checked.)
3. Do one of the following:
   - For all messages except File stored on volume that does not support ACLs, select a test file that is stored on a volume that supports ACLs.
   - For File stored on volume that does not support ACLs, select a test file that is stored on a volume that does not support ACLs.

4 In the Template file list option, enable the File template that lists the files that you want to examine. See “Template file list” on page 114.

5 For the following messages, complete the corresponding steps:

Message name	Steps
Additional ACL entry	1 Select a test file that is stored on a volume that supports ACLs. 2 In Windows Explorer, add a valid group with Read privileges to the file. Do not add the group to the ACL sublist in the template.
Different ACL entry	1 Select a test file that is stored on a volume that supports ACLs. 2 In Windows Explorer, add a valid group with Read privileges to the file. 3 In the Sublist Editor for the ACL sublist, add the same group with All privileges to the File template.
Missing ACL entry	1 Select a test file that is stored on a volume that supports ACLs. 2 In the Sublist Editor for the ACL sublist, add a valid group with Read privileges to the File template. Do not add the group to the file stored on a volume that supports ACLs.
Account specified in template does not exist on system	1 Select a test file that is stored on a volume that supports ACLs. 2 In the Template Editor for the ACL sublist, add an invalid group with Read privileges to the File template.
File stored on volume that does not support ACLs	1 Select a test file that is stored on a volume that does not supports ACLs. 2 In the Template Editor, add the test file. 3 In the Sublist Editor for the ACL sublist, add a valid group with Read privileges to the file.
Additional SACL Entry	1 Select a test file that is stored on a volume that supports ACLs. 2 In Windows Explorer, direct the system to audit all success and failure events by a valid user. 3 In the Sublist Editor, Ensure that the user is not listed in the Auditing ACL sublist for the test file. See “Editing an Auditing ACL sublist” on page 120.

Message name	Steps
Different SACL Entry	1 Select a test file that is stored on a volume that supports ACLs. 2 In Windows Explorer, direct the system to audit all success and failure events by a valid user. 3 In the Sublist Editor, edit the Auditing ACL sublist for the test file and add the same user. Specify that the system should audit only read success and failure events.
Missing SACL Entry	1 Select a test file that is stored on a volume that supports ACLs. 2 In the Sublist Editor, edit the Auditing ACL sublist for the test file and add an invalid user. Specify that the system should audit only read success and failure events.

To protect your computers

- Do one of the following:
  - For authorized changes, update the File templates (TU) in the console grid.
  - For unauthorized changes, use the Correct feature in the console grid to reverse the changes. Then run the Changed file (signature) check. See “Changed file (signature)” on page 128.

Hidden files and folders

This security check reports any hidden files in the folders or volumes that you specify in the file list. Intruders sometimes hide files and folders to access and report critical information.

The check returns the following messages:

Message name	Title	Class
HIDDEN_DIRECTORY	Hidden folder	0
HIDDEN_FILE	Hidden file	0

To demonstrate the check

1. Create a test file.
2. In Windows Explorer, right-click the test file, then click **Properties** > **General**.
3. Check **Hidden**, then click **OK**.

4 In a demo policy, disable all checks in the File Attributes module except hidden files and folders.

5 In the Hidden files and folders security check, add the test file to the name list.

6 Run the demo policy and verify that the appropriate message is reported

7 Repeat steps 2–5, substituting a test folder for the test file.

To protect your computers

- Remove any hidden files or folders that do not belong on the computer.

File and folder permissions

This security check reports file and folder permissions of files that are specified in the file list. Specify drive letters and full file path names. If you enter a folder that is stored on a FAT volume, the check reports that Everyone has Full Control for the folder and its subfolders. Full Control means that anyone can modify or delete reported files and folders unless specifically denied access.

The check returns the following messages:

Message name	Title	Class
DIRECTORY_PERMS	Folder permissions	0
FILE_PERMS	File permissions	0

To demonstrate the check

1 Create a test file on an NTFS volume.

2 In a demo policy, disable all checks in the File Attributes module except File and folder permissions.

3 In Windows Explorer, right-click a test file on an NTFS volume, then click **Properties** and note its permissions.

4 In the File template, check **Enable ACL Checking** for the test file, then click **Save**.

5 In the Template File List option, enable the File template that lists the files that you want to examine. See “Template file list” on page 114.

6 In the File and folder permissions check, add the test file to the name list, then click **OK**.

7 Run the demo policy and verify that the appropriate message is reported.

8 Repeat steps 2–6, substituting a test folder for the test file.

To protect your computers

- Do one of the following:
  - For authorized changes, manually update the File template.
  - For unauthorized changes, restore the correct permissions.
  - Run the Changed file (signature) check. See "Changed file (signature)" on page 128.

Files giving all users Full Control

This security check reports files and folders that grant Full Control to the Everyone security group.

Anyone can modify or delete reported files and folders unless specifically denied access.

Specify files or folders to examine in the Files/folders to examine name list.

The check returns the following message:

Message name	Title	Class
FILES_WITH_ALL_ACCESS	File or folder giving all users Full Control	1

To demonstrate the check

1. Create a test file.
2. Verify that Everyone has Full Control on the test file.
   In Windows Explorer, right-click the test file, then click **Properties** > **Security**. If Everyone does not already have Full Control permissions, check **Allow**.
3. In a demo policy, disable all checks in the File Attributes module except Files giving all users Full Control.
4. In the File template, load the test file. See "To load attributes of a single file" on page 115.
5. Enable the template.
6. Run the demo policy on the agent computer.
7. Verify that the policy run reports File or folder giving all users Full Control.
8. Repeat steps 1–7, substituting a test folder for the test file.

To protect your computers

- Do one or more of the following:

- Remove files that all users should be able to control from the name list.
- Assign authorized permissions to the reported files and folders.
- Run the Changed file (signature) check. See "Changed file (signature)" on page 128.

Allow any privileged account

This option directs the File ownership and File ACL security checks to ignore ownership changes that do not compromise security.

In most situations, if the template specifies account ownership by Administrator, ownership by any privileged account is accepted. Privileged accounts belong to the Administrators security group.

The option accommodates variations in ownership between different versions or installations of the same operating system while still using the same templates.

Every file and folder on an NTFS file system has an owner. Only the owner account can access the object and modify its properties. Important files on your computer should be owned by privileged accounts.

Do not notify if file permissions are increased in security

This option directs the File ACL check to report only changes that decrease security by expanding permissions on files. If the option is disabled, the File ACL check reports all changes to file permissions.

Expanded file permissions (which decrease security) are usually more of a security concern than removed permissions (which increase security). This check lets you limit your review to changes that decrease security.

Do not notify if User/Group in ACL is not on system

This option directs the ACL check to ignore user names in the template ACL sublist that do not exist on the computer. If the option is disabled, the File ACL check reports that these users do not exist on the computer.

If template maintenance is done on a different schedule than system maintenance, this option lets you limit your review to users on the computer.

File Watch

The File Watch module reports changes to files since the last snapshot update and violations of template settings.

- Most module security checks use File Watch templates, which define the files, folders, and operating systems that are watched, the depth of folder traversal, and the types of changes that are reported. These templates have .fw file extensions. See "Editing the File Watch template" on page 136.
- The Malicious files security check uses Malicious File Watch templates, which define known attack files and signature patterns. These files have .mfw extensions. See "Editing Malicious File Watch templates" on page 146.
- The Changed file (signature) security check uses File Signatures templates to compare file signatures on the agent with signatures that are stored in templates on Symantec ESM 5.1 and 5.5 managers. These templates have .fs file extensions. See "Editing the File Signatures template" on page 141.

You can use some File Watch messages to update snapshot or template files to match current agent settings. Updateable messages are identified as TU or SU types in the descriptions of checks that use them. See "Updating template and snapshot files in messages" on page 42.

Common File Watch messages

File Watch messages that are not mapped to specific security checks are generated by running the following:

- The function that creates the baseline snapshot file the first time the File Watch module is run on an agent.
- Security checks and options that use templates (the Files/folders to watch option, the Malicious files check, and the Changed file (signature) check.)
- Security checks that cannot locate, and therefore cannot use, a file or folder that is listed in a template.

The following messages are not mapped to specific security checks:.

Message name	Title	Class
SNAPSHOT_ TAKEN	Snapshot taken	0
NO_TEMPLATE	No template specified	4
FILE_NOT_CHECKED	File not checked	0

Files/directories to watch

Use this option to enable or disable *.fw template files that specify files, folders, and operating systems to watch.

Editing the File Watch template

The File Watch template specifies:

- Files and folders for the module to watch.
- Depth of folder traversal.
- Types of changes to evaluate.

Do not edit the File Watch template that is installed with Symantec ESM. Instead, add your own.

To add a new File Watch template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Available template types list, click **File Watch - all**.
3. In the Template file name text box, type a template name of no more than eight characters, without a file extension. The .fw extension is added automatically.
4. Press **Enter** to save the template and open the Template Editor.

To add a row to a File Watch template

1. If the Template Editor is not already open, double-click the name of the template that you want to edit in the Templates branch of the enterprise tree.
2. Click **Add Row**.
3. Add one or more entries to the OS/Rev sublist. See "To add a row to an OS/Rev sublist" on page 137.
4. Add one or more entries to the Excludes sublist. See "To add a row to an Excludes sublist" on page 138.
5. In the File/Folder to watch field of the row that you added in step 2, replace <NEW> with the path name of the file or folder that you want to monitor.
6. Click the Depth field, then select the value that defines how far down the directory tree you want the module to travel to watch for changes.

7 Check or uncheck the following check boxes:

Ownership	Report items that changed ownership after the last snapshot update.
New	Report items that were added after the last snapshot update.
Removed	Report items that were removed after the last snapshot update.

8 Click the Permissions field, then select **None**. (The Permissions field is used for UNIX computers only.)

9 Click the Signature field, then select the type of file signature that you want to watch for. This field is used only by the Changed files (signatures) check, which uses the signature type in the File Signatures template.

10 Click **Save**. To add another row, repeat steps 2–9.

11 Click **Close** to exit the Template Editor.

To add a row to an OS/Rev sublist

1 In the Template Editor, click the **OS/Rev** button on the row that you are editing.

2 In the Template Sublist Editor, click **Add Row**.

3 Do one of the following:

- Check **Exclude** to exclude the specified operating system and revision for security checks that use the File Watch template.
- Uncheck **Exclude** to include the specified operating system and revision for security checks that use the File Watch template.

4 Click the OS field (initially ALL), then select one of the following options:

- All (All platforms)
- UNIX (All UNIX platforms)
- NT (All NT platforms)
- WIN2K (All WIN 2000 platforms)
- WINXP (All WIN XP platforms)
- WIN2K3
- aix-rs6k
- hpux-hppa
- irix-mips
- ncr-x86
- osf1-axp
- solaris-sparc

- sunos-sparc
- sequent-x86
- redhat-x86
- redhat-s390
- nt-ix86

5 In the Revision field, replace <NEW> with the version of the operating system revisions that you want to exclude or include. Use these conventions to identify multiple revisions:

- ALL for all releases and revisions.
- A leading minus (-) sign for the specified revision and all earlier revisions. For example, -5.0
- A leading plus (+) sign for the specified revision and all later revisions. For example, +5.0

6 Click **Apply**. To add another row, repeat steps 2–6.

7 Click **Close** to exit the Template Sublist Editor.

To add a row to an Excludes sublist

1 In the Template Editor, click **Excludes**.

2 In the Template Sublist Editor, click **Add Row**.

3 In the File/folder to exclude field, replace <NEW> with the name of the file or subfolder that you want to exclude from checks that are defined on the same template row as the Excludes sublist.

For example, if the template row defines File Watch checks for users, you would enter a file or subfolder within that folder in the sublist.

4 Check or uncheck one or more of the following check boxes to indicate whether the associated change is to be excluded or included for reports on the specified file or folder:

- Ownership
- Permissions
- Signature
- New
- Removed

5 Click **Apply**.

Repeat steps 2–5 to add another row.

6 Click **Close** to exit the Template Sublist Editor.

Changed files (ownership)

This security check reports changes in folder and/or file ownerships on specified volumes. The related Ownership check box must be checked in the File Watch template.

You can use the Excludes sublist in the File Watch template to exclude specified subfolders or files from the check.

The check returns the following message:

Message name	Title	Type	Class
DIFF_OWN	File ownership modified	SU	1

To demonstrate the check

1. In a demo policy, disable all checks in the File Watch module of the demo policy except Changed files (ownership).
2. If you have not already done so, create a test folder and text file on a selected NTFS volume.
3. In the Template Editor, edit the File Watch template to monitor only the test folder on the selected volume and check **Ownership**.
4. If the module has never been run on the agent, run the demo policy to create the snapshot file.
5. Change the owner of the text file to a different user.
6. Run the demo policy on the agent.
7. Verify that File ownership modified is reported.

To protect your computers

- Do one of the following:
  - For an authorized change, update the snapshot in the console grid.
  - For an unauthorized change, restore the file or folder to its rightful owner, then rerun the check.

Changed files (signature)

This security check reports files with CRC, MD5, or combined CRC and MD5 file signatures that do not match the signatures and signature types that are defined in the File Signatures template.

This check compares file signatures on the agent computer with signatures in templates on a manager. The Invalid signature check compares current file signatures with snapshot records on the agent. See "Invalid signature" on page 152.

By checking file signatures against templates on a manager, you can verify that all agents have identical versions of critical files. This also protects signature data from tampering by users who can access agents but not managers.

You must create a new *.fs File Signatures template before you can use the check's name list to enable or disable the template.

This check returns the following messages:

Message	Title	Type	Class
SIG_NOTMATCH	File signature does not match template	TU	1
SIGTYPE_ NOTMATCH	File signature type does not match template	TU	0
FILE_NOTEXIST	Mandatory file does not exist		3

To demonstrate the check

1. In a demo policy, disable all checks in the File Watch module except Check File Signatures Against Template.
2. Use the name list to enable the File Signatures template that lists the files that you want to check.
3. Launch the related application and change the contents of a test file. For example, if the test file is a text file, launch Notepad and add some text.
4. Run the demo policy on the agent computer.
5. Verify that File signature does not match template is reported.

To protect your computers

- Do one of the following:
  - For each authorized change, update the template in the console grid.
  - For each unauthorized change, restore the file or folder from a backup or from the original distribution media.

Editing the File Signatures template

In the Files Signatures template, specify the files that you want to monitor for changes. Three methods of specifying files are available:

- Add File: Individual file on an agent. See "To load signature information for an individual file" on page 141.
- Add Folder: All files in a specified folder. You may also include all files in all subfolders or all files in a specified number of subfolders. See "To load signature information for all files in a folder" on page 142.
- Add Entry: Individual files with specific criteria. This method is seldom used because it does not generate file signatures as the other methods do. See "To manually enter signature information about a single file" on page 142.

To add a new File Signatures template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Create New Template dialog box, select **File Signatures - all**.
3. Type a new template name of no more than eight characters, without a file extension. A .fs extension is automatically added.
4. Press **Enter**.
5. Add one or more rows.
6. Click **Save**.
7. Click **Close** to exit the Template Editor.

To load signature information for an individual file

1. If the Template Editor is not already open, double-click the name of the template in the enterprise tree.
2. In the Template Editor, click **Add File**.
3. In the Add Items to Template dialog box, select an agent.
4. Type the path and name of the file that you want to monitor.
5. Press **Enter**.
   To add another file using this method, repeat steps 2–4.
6. Click **Save**.
   To load signature information for another file, repeat steps 2–6. You can also load file information using the Add Directory or Add Entry methods.
7. Click **Close**.

To load signature information for all files in a folder

1. If the Template Editor is not already open, double-click the name of the template in the enterprise tree.
2. In the Template Editor, click **Add Directory**.
3. In the Add Hierarchical Items to Template dialog box, select an agent name.
4. Type the path and name of the parent folder. Do not specify an empty folder.
5. Select the option that describes the level of subfolders and files that you want to load.
   - **This item and all subordinates**
   - **This item only (no subordinates)**
   - **Include <number> subordinate levels**
6. Click **OK**.
   To add another file using this method, repeat steps 2–6.
7. Click **Save**.
   To load signature information for all files in another folder, repeat steps 2–7. You can also load file signature information using the Add File method.
8. Click **Close**.

To manually enter signature information about a single file

1. If the Template Editor is not already open, double-click the name of the template in the enterprise tree.
2. In the Template Editor, click **Add Entry**.
3. Click the Agent name field, then select the agent that has the folder.
4. In the Item to add text box, type the folder path for the module.
5. Select the option that describes the level of subordinate folders and files that you want to load from the Items to include group. Each subordinate level includes the files that are located within that level.

   For example, this figure displays settings to add all files, including those in subfolders, of the GS0100 agent's c:\security folder to the template:
6. Replace <NEW> with the agent name, file name, and file signature.
7. In the Required field, select one of the following:
   - **Optional** File existence is optional.
   - **Mandatory** File must exist.

8 In the Signature Type field, select the signature type that you want to use to watch for changes. By default, the File Watch module loads new entries with MD5 signatures.

- **CRC** 16-bit signature
- **MD5** 128-bit signature
- **CRC+MD5** Combined CRC and MD5

When you change the Signature Type value after a file record is loaded, the check reports that fact and lets you update the file signature.

9 Click **Save**.
To add another row, repeat steps 2–6.
You can now add files using the Add File or Add Directory methods.

10 Click **Close**.

New files

This security check reports new folders and/or files on specified volumes that were added after the last snapshot update. The related New check box must be checked in the File Watch template.

You can use the Excludes sublist in the File Watch template to exclude specified subfolders or files from the check.

The check returns the following message:

Message name	Title	Type	Class
NEW	New directory or file	SU	0

To demonstrate the check

1 In a demo policy, disable all checks in the File Watch module of the demo policy except New files.

2 If you have not already done so, create a test folder on a selected NTFS volume.

3 If the module has never been run on the agent, run the demo policy to create the snapshot file.

4 Add a text file to the test folder.

5 Add a test subfolder to the test folder.

6 Run the demo policy on the agent computer and verify that New directory or file is reported.

To protect your computers

- For each reported change, do one of the following:
  - For an authorized addition, update the snapshot in the console grid.
  - For an unauthorized addition, delete the file or folder, then rerun the check.

Removed files

This security check reports folders and/or files on watched volumes that were deleted after the last snapshot update. This check requires that the related Removed check box in the File Watch template be checked.

You can use the Excludes sublist in the File Watch template to specify subfolders or files that you want to exclude from the check.

This check returns the following message:

Message name	Title	Type	Class
REMOVED	Directory or file removed	SU	0

To demonstrate the check

1. In a demo policy, disable all checks in the File Watch module except Removed files.
2. If you have not already done so, create a test folder on an NTFS volume.
3. If you have not already done so, run the verification steps to update the snapshot for the new text file. See “New files” on page 143.
4. Remove the text file from the test folder.
5. Run the demo policy and verify that Directory or file removed is reported.

To protect your computers

To protect your computers

- Do one of the following:
  - For an authorized deletion, update the snapshot in the console grid.
  - For an unauthorized deletion, restore the file or folder from a backup or from the original distribution media, then rerun the check.

Malicious files

This security check reports files that match file names or attack signatures that are defined in Malicious File Watch *.mfw template files. These templates are used only by the Malicious files check.

In the check's name list, enable or disable Malicious File Watch *.mfw templates.

The check returns the following messages:

Message	Title	Class
MALICIOUS_FILE	Possible malicious file found	2
MALICIOUS_ RUN_PROCESS	Possible malicious run process found	2
MFW_ACCESS_ BLOCKED	File access blocked	0
MFW_TEMPLATE_ ERR	MFW template error	1

Warning: Do not attempt to demonstrate the messages that are produced by this check. These messages indicate the presence of files and processes that can be used for malicious purposes on your computer.

To protect your computers

- Implement the latest counter-measures for known security vulnerabilities. You can obtain information about current security vulnerabilities from Symantec Corporation and other security information clearing houses on the Internet:

Organization	URL
Symantec Security Response	http://securityresponse.symantec.com
CERT Coordination Center	http://www.cert.org
Center for Education and Research in Information Assurance and Security (CERIAS)	http://www.cerias.purdue.edu
Computer Incident Advisory Capability (CIAC)	http://www.ciac.org/ciac/
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org
InfoSysSec	http://www.infosyssec.com

Organization	URL
Internet/Network Security	http://netsecurity.about.com
Microsoft Corporation	http://www.microsoft.com
NTBugtraq	http://www.ntbugtraq.com
NTSecurity Net	http://www.ntsecurity.net
SecurityFocus	http://www.securityfocus.com
Storm Center	http://www.incidents.org
System Administration, Networking and Security (SANS Institute) Top Twenty	http://www.sans.org/top20.htm

Editing Malicious File Watch templates

Do not edit the Malicious File Watch templates that are installed with Symantec ESM. Instead, add your own and edit them. See “To add a new Malicious File Watch template” on page 147.

The File Watch module includes several default Malicious File Watch templates with file names that indicate the operating systems and vulnerabilities that they report.

File name	System	Reports
w2k.mfw nt.mfw unix.mfw	Windows 2000, XP Windows NT UNIX	Attack signatures for files and processes that are used by trojan horse programs to mount denial of service attacks.
ntnipc.mfw	Windows	Files that have been targeted in attacks on e-commerce and e-finance/banking businesses (NIPC advisory 01-003).
nthacktl.mfw	Windows	Files that are often used for hacking but may also have legitimate uses.
unixhide.mfw	UNIX	Files that are used by the Hide rootkit, a set of “back door” programs that lets an attacker gain privileged access to a system, modify system commands, and install trojan horse programs.

File name	System	Reports
lnxadore.mfw	RedHat Linux	Files that indicate infection by the Adore worm. Worms search for vulnerabilities, gather information, deny services, and/or install rootkits. The Adore worm spreads to other systems by exploiting LPRng, rpc-statd, wu-ftpd, and BIND vulnerabilities.
lnxlion.mfw	RedHat Linux	Files that indicate infection by the Lion worm. The Lion worm installs the t0rn rootkit and spreads to other systems by exploiting a BIND TSIG vulnerability.
lnxt0rn.mfw	RedHat Linux	Files that indicate the t0rn rootkit. A rootkit is a set of “back door” programs that lets an attacker gain privileged access to a system, modify system commands, and install trojan horse programs. The t0rn rootkit is installed by the Lion worm.

To add a new Malicious File Watch template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Available template types list, click **Malicious File Watch - all**.
3. In the Template file name text box, type a template name of no more than eight characters, without a file extension. The .mfw extension is automatically added.
4. Press **Enter** to save the template and open the Template Editor.

To add a row to a Malicious File Watch template

1. If the Template Editor is not already open, double-click the name of the template that you want to edit in the Templates branch of the enterprise tree.
2. Click **Add Row**.
3. In the Name field of the new row (added to the bottom of the list), replace <NEW> with the name of the attack that is associated with the malicious files that you are defining.
4. In the Description field, replace <NEW> with a description of the attack.
5. Add rows to the OS/Rev sublist. See “To add a row to an OS/Rev sublist” on page 148.
6. Add rows to the Folders sublist. See “To add a row to a Folders sublist” on page 149.

7. Add rows to the File Type sublist. See "To add a row to a File Type sublist" on page 149.
8. Add rows to the Signature sublist. See "To add a row to a Signature sublist" on page 150.
9. Add rows to the Signature Patterns sublist. See "To add a row to a Signature Patterns sublist" on page 151.
10. Add rows to the File Extension. See "To add a row to a File Extension sublist" on page 151.
11. Click **Save**.

    To add another row, repeat steps 2–6.
12. Click **Close** to exit the Template Editor.

To add a row to an OS/Rev sublist

1. In the Template Editor, click the OS/Rev sublist button (initially 0).
2. In the Template Sublist Editor, click **Add Row**.
3. Check **Exclude** to exclude the specified operating system and revision, or uncheck **Exclude** to include the operating system and revision.
4. In the new row, click the OS field (initially ALL).
5. Select the value that describes the operating system that you want to exclude or include.
6. In the Revision field, replace <NEW> with the version of the operating system revisions that you want to exclude or include.

   For multiple revisions use:

   - ALL for all releases and revisions.
   - A leading minus (-) sign for the specified revision and all earlier revisions. For example, -5.0
   - A leading plus (+) sign for the specified revision and all later revisions. For example, +5.0
7. Click **Apply**.

   To add another row, repeat steps 2–6.
8. Click **Close** to exit the Template Sublist Editor.

To add a row to a Folders sublist

1. In the Template Editor, click the Folders sublist button (initially 0).
2. In the Template Sublist Editor, click **Add Row**.
3. In the Folder to watch field, replace <NEW> with the name of a volume or folder.
4. If you do not want to watch all sub-items of the volume or folder, click the Depth field, then click **Item Only**.
5. Click **Apply**.
   To add another row, repeat steps 2–6.
6. Click **Close** to exit the Template Sublist Editor.

To add a row to a File Type sublist

1. In the Template Editor, click **File Type**.
2. In the Template Sublist Editor, click **Add Row**.
3. Check **Exclude** if you intend to specify file types to exclude from malicious files security checks, or uncheck **Exclude** if you intend to specify file types to include.
4. Click the File Type field (initially All), then select a file type:
   - **All**
   - **Directory**
   - FIFO (UNIX only)
   - block special (UNIX only)
   - character special (UNIX only)
   - executable (UNIX only)
   - regular file (UNIX only)
   - symbolic link (UNIX only)
   - socket (UNIX only)
   - **executable program**
   - **file extension**
   - **DLL programs**
5. Click **Apply**.
   To add another row, repeat steps 2–5.
6. Click **Close** to exit the Template Sublist Editor.

To add a row to a Signature sublist

1. In the Template Editor, click **Signature**.
2. In the Template Sublist Editor, click **Add Row**.
3. In the Signature ID field, replace <NEW> with a name or number that uniquely identifies the entry.
4. Click the Signature Type field, then select one of the following signature types:
   - **Bytes** One ASCII character per byte. You can also use the \x escape sequence to specify any byte sequence as a hexadecimal value in the format \xn or \xnn, where x is not case sensitive and n is one of the following digits: 0123456789abcdef
   - **Word** A 16-bit word sequence. A hexadecimal value, including up to four hexadecimal digits per word, preceded by the \x escape sequence.
   - **DWord** A 32-bit double word sequence. Double word as a hexadecimal value, including up to eight hexadecimal digits per word, preceded by the \x escape sequence.
   - **File Name** A case-sensitive file path name.
   - **FILE NAME** A case-insensitive file path name.
5. In the Signature Pattern field, replace <NEW> with a signature pattern or file name. The File Name is compared to FILE NAME patterns at the end of each file path.

   Note: If you do not begin path names with two back slashes (\\), or UNIX path names with a forward slash (/), they will be added. For example, if you specify the pattern lib/lib on a UNIX system, the module reports matches for /lib/lib as well as for /usr/lib/lib, but not for /usr/mylib/lib or /lib/lib/subdir.

   Escape sequences for byte sequence signature patterns:
   - \a (bell)
   - \b (backspace)
   - \f (formfeed)
   - \n (new line)
   - \r (carriage return)
   - \t (horizontal tab)
   - \v (vertical tab)
   - \x (hexadecimal escape sequence followed by n or nn, where n is one of these hexadecimal digits: 0123456789abcdef)

6 Click **Apply**. To add another row, repeat steps 2–6.

7 Click **Close** to exit the Template Sublist Editor.

To add a row to a Signature Patterns sublist

1 In the Template Editor, click **Signature Patterns**.

2 In the Template Sublist Editor, click **Add Row**.

3 In the Probability field, enter a number between 1 and 100 that defines the probability that a file containing all of the signatures listed in the Signature IDs column does indicate the presence of a malicious file on your computer.

4 In the Message field, replace <NEW> with text that explains how the file that is identified by the Signature ID is used by attackers.

5 In the Signature IDs column, replace <NEW> with Signature IDs from the Signature sublist to associate rows in this sublist with Signature sublist rows on the same template row. Separate multiple Signature ID values by commas. For example, 2,5,6.

6 Click **Apply**. To add another row, repeat steps 2–6.

7 Click **Close** to exit the Template Sublist Editor.

To add a row to a File Extension sublist

1 In the Template Editor, click **File Extension**.

Note: The file extension file type must not be excluded in a File Type sublist entry on the same template row.

2 In the Template Sublist Editor, click **Add Row**.

3 Check **Include** to include files with the specified extension or uncheck **Include** to exclude the files when the module runs.

4 In the Extension field, replace <NEW> with the file extension that identifies files that are to be included or excluded.

Invalid signature

This security check reports files with signatures that changed after the last snapshot update. differences between current values and the most recent snapshot update for MD5 and/or CRC signatures on specified files and folders.

The signature type is specified in the Signature field of the File Watch template.

You can use the Excludes sublist in the File Watch template to exclude specified subfolders or files from the check.

The check returns the following message:

Message name	Title	Type	Class
MODIFIED	File modified	SU	1

Note: The File Watch module cannot perform signature checks on the unencrypted contents of Windows 2000 encrypted files. Instead, it examines signature checks of the raw, encrypted versions of these files.

This lets the module report changes to file signatures even when the contents of specified files have not changed. For example, the check reports signature changes for any file that has been encrypted or decrypted, or that has had user or file recovery agent changes.

To demonstrate the check

1. In a demo policy, disable all checks in the File Watch module except Invalid signature.
2. If you have not already done so, create a test folder and text file on a selected NTFS volume.
3. In the Template Editor, edit the File Watch template to monitor only the test folder on the selected volume, and verify that the Signature value is not None.
4. If the module has never been run on the agent, run the demo policy to create the snapshot file.
5. Replace a word in the created text file with another word that contains the same number of characters.
6. Run the demo policy on the agent computer and verify that File modified is reported.

To protect your computers

- Do one of the following:
  - For an authorized change, update the snapshot in the console grid.
  - For an unauthorized change, restore the file or folder to its rightful owner, then rerun the check.

Integrated Command Engine (ICE)

The Integrated Command Engine (ICE) is a unique, extensible module in the Dynamic Assessment policy. It contains no security checks or templates, but gives users the ability to integrate user scripts and executables and with Symantec ESM. In effect, they become the module's security checks. Because the ICE module is so different from all other modules, it is documented in the Appendix. See "Integrated Command Engine (ICE)" on page 267.

Login Parameters

The Login Parameters module reports problems if the previous user name is displayed on the Logon screen, if shutdown is possible without logon, and if automatic logons are allowed. It also reports old or unused accounts and accounts that are not locked out after a specified number of failed logon attempts.

Warning: Securing your computers from logon vulnerabilities may require modifying the Windows registry. Incorrectly changing the registry can cause serious, system-wide problems. Update the Windows Emergency Repair disk before making any changes.

Account lockout threshold

This security check reports accounts that are not locked out after a specified number of bad logon attempts.

Account lockout is a global setting. When you change the setting for one user, all users inherit the new setting. Domain settings override local settings.

Specify your policy's account lockout threshold in the Bad logon attempts text box. The default value is 5.

The check returns the following messages:

Message name	Title	Class
ACCOUNT_LOCKOUT_DISABLED	Account lockout is disabled	4
FAILED_ATTEMPTS_TOO_HIGH	Number of bad logon attempts is higher than your policy	1
FAILED_ATTEMPTS_TOO_LOW	Number of bad logon attempts is lower than your policy	1

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Account lockout threshold.
2. Do one of the following.

Message title	Steps
Account lockout is disabled	Windows 2000/XP: 1 Set the local and domain Account Lockout Policy values to 0. 2 Run secedit /refreshpolicy machine_policy. After you have reported this message, reset the value to 1 and refresh the policy. Windows NT: ◆ In the User Manager, select No account lockout in the Account Policy. After you have reported this message, select Account lockout in the Account Policy.
Number of bad logon attempts is higher than your policy	In the Account lockout threshold check, set the Bad logon attempts text box value to 100.
Number of bad logon attempts is lower than your policy	In the Account lockout threshold check, set the Bad logon attempts text box value to 1.

3. Run the demo policy.
4. Verify that appropriate message is reported.
5. Repeat steps 2–4 using a different procedure until each message has been reported.

To protect your computers

- Do one of the following:
  - Windows 2000/XP: In the Account Lockout Policy, specify an Account lockout threshold of no more than 5.
  - Windows NT: In the User Manager's Account Policy, Ensure that Account lockout is selected and specify a value of no more than 5 in the Lockout after ... bad logon attempts field.

Account lockout duration

This security check reports a problem when the account lockout feature specifies fewer than the number of minutes specified in your policy.

In the Time (minutes) text box, type the number of lockout minutes that is authorized by your policy. The default value is 60. If accounts are to remain locked until unlocked by the system administrator, type 0.

Lockout duration is a global setting. When you change it for one user, all users inherit the new setting. Domain settings override local settings.

The check returns the following message:

Message name	Title	Class
LOCKOUT_TIME_TOO_LOW	Lockout time too low	1

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Account lockout duration.
2. Do one of the following:
   - Windows 2000/XP: In the Account Lockout Policy, set the local and domain Account lockout duration to 1, then run secedit /refreshpolicy machine_policy to apply the new setting to the agent immediately, or wait for the refresh period to end (90 minutes plus or minus 30 minutes).
   - Windows NT: In the User Manager's Account Policy, set the Duration ... minutes field to 1.
3. Run the demo policy.
4. Verify that Lockout time too low is reported.

To protect your computers

- Do one of the following:
  - Windows 2000/XP: In the Account Lockout Policy, set the local and domain Account lockout duration to at least 60 minutes.
  - Windows NT: In the User Manager's Account Policy, set the Duration ... minutes field to at least 60 minutes.

Bad logon counter reset

This security check reports a problem if the lockout time is set for less than the amount that you specify. Domain settings override local settings.

In the Time (minutes) text box, type the number of minutes that an account should be locked out. The default value is 20.

Counter reset time is a global setting. When you change it for one user, all users inherit the new setting

The check returns the following message:

Message name	Title	Class
COUNTER_TIME_TOO_LOW	Counter reset time too low	1

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Bad logon counter reset.
2. Do one of the following:
   - Windows 2000/XP: In the Account Lockout Policy, set the local and domain Reset account lockout counter after setting to 1, then run secedit /refreshpolicy machine_policy.
   - Windows NT: In the User Manager's Account Policy, set the Reset count after ... minutes field to 1.
3. Run the demo policy.
4. Verify that Counter reset time too low is reported.

To protect your computers

- Do one of the following:
  - Windows 2000/XP: In the Account Lockout Policy, set the local and domain Reset account lockout counter to at least 20 minutes.
  - Windows NT: In the User Manager's Account Policy, set the Reset count after ... minutes field to at least 20 minutes.

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Legal notice.
2. Run the demo policy.
3. Notice which message title is reported.
4. Change the contents of:
   - Windows 2000/XP: In Security Options, Message text and Message title for users attempting to log on.
   - Windows NT: In the Winlogon registry key, LegalNoticeCaption and LegalNoticeText.

   See Legal notice text.
5. Run the demo policy.
6. Verify that the notice which was not reported in step 2 is reported now.

Legal notice text

To specify the title and text of a legal notice in Windows 2000/XP

1. In the Local Security Policy, click Local Policies > Security Options.
2. Type text in the Message text and Message title for users attempting to log on fields.
3. Run secedit /refreshpolicy machine_policy to apply the new setting to the agent immediately, or wait for the refresh period to end (90 minutes plus or minus 30 minutes).

To specify the caption and text of a legal notice in Windows NT

1. Run regedit.
2. Click **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Windows NT** > **CurrentVersion** > **Winlogon**.
3. Type text in the LegalNoticeCaption and LegalNoticeText fields.

To remove the text of legal notice title and message fields

- Follow the steps above for your operating system except delete the text in step 3.

To protect your computers

- Define and enable a legal access notice on the agent computer.

Expired logon hours disconnect (Windows NT/2000)

This security check for domain controllers reports a problem when users are not automatically disconnected from the network when authorized logon hours expire.

If users are not forcibly disconnected from the network when their logon times expire, they can remain connected for as long as they like.

The check returns the following message:

Message name	Title	Class
NO_FORCIBLE_LOGOUT	System without forcible disconnect	1

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Expired logon hours disconnect.
2. Run the policy on the agent.
   If System without forcible disconnect is reported, the demonstration is complete. If it is not reported, continue to step 3.
3. Do one of the following:
   - Windows 2000 domain controller: In the Domain Security Policy, click **Local Policies** > **Security Options**, then enable Automatically log off users when logon time expires. Run secedit /refreshpolicy machine_policy to apply the new setting to the agent immediately, or wait for the refresh period to end (90 minutes plus or minus 30 minutes).
   - Windows NT domain controller: In the User Manager, click **Policies** > **Account**, then check Forcibly disable remote users from server when logon hours expire.
4. Run the policy on the agent.
5. Verify that System without forcible disconnect is reported.

To protect your computers

- ◆ For strict security, set domain policies to disconnect users when authorized logon hours expire.

Last user name hidden

This security check reports a problem when the last input user name is displayed in the Logon screen. Hide the last user name to protect it from unauthorized use.

If the user name of the most recently accessed account appears in the Logon screen, the system gives away half of the user name/password security combination that is intended to protect the account from unauthorized access.

The check returns the following message:

Message name	Title	Class
USERID_NOT_HIDDEN	Last user ID is not hidden	1

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Last user name hidden.
2. Run the policy on the agent.
   If Last user ID is not hidden is reported, the demonstration is complete. If it is not reported continue to step 3.
3. Do one of the following:
   - Windows 2000 domain controller: In the Domain Security Policy, click **Local Policies** > **Security Options**, then enable Do not display last user name in logon screen. Run secedit /refreshpolicy machine_policy to apply the new setting to the agent immediately, or wait for the refresh period to end (90 minutes plus or minus 30 minutes).
   - Windows NT domain controller: In the System Policy Editor, click **File** > **Open Registry**, double-click **Local Computer**, open the Windows NT System book and the Logon book, then uncheck Do not display last logged on user name.
4. Click **OK**.
5. Run the policy on the agent.
6. Verify that Last user ID is not hidden is reported.

To protect your computers

- Do not display the previous user name in the Logon screen.

Shutdown without logon

This security check for domain controllers reports a problem if shutdown is enabled in the Logon screen.

If shutdown is allowed in the Logon screen, a Shutdown button is available on the Logon screen and anyone can shut down the system without logging on. This allows anyone to interrupt system operations.

The check returns the following message:

Message name	Title	Class
SHUTDOWN_FROM_LOGON	Shutdown from Logon screen is enabled	1

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Shutdown without logon.
2. Run the policy on the agent.

   If Shutdown from Logon screen is enabled is reported, the demonstration is complete. If it is not reported continue to step 3.
3. Do one of the following:
   - Windows 2000 domain controller: In the Local Security Policy, click **Local Policies** > **Security Options**, then enable Allow system to be shut down without having to log on. Run secedit /refreshpolicy machine_policy to apply the new setting to the agent immediately, or wait for the refresh period to end (90 minutes plus or minus 30 minutes).
   - Windows NT domain controller: In the System Policy Editor, click **File** > **Open Registry**, double-click **Local Computer**, open the Windows NT System book and the Logon book, then check Enable shutdown from Authentication dialog box.
4. Run the policy on the agent.
5. Verify that Shutdown from Logon screen is enabled is reported.

To protect your computers

◆ Do not allow shutdown from the Logon screen.

Autologon disabled

This security check for domain controllers reports user accounts that can avoid logging on by using a default name and password.

The check returns the following message

Message name	Title	Class
AUTOLOGON_ENABLED	Autologon is enabled	4

To demonstrate the check

1. In a demo policy, disable all checks in the Login Parameters module except Autologon disabled.
2. Run regedt32 and go to HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/ Windows NT/Current Version/Winlogon.
3. Specify a default user name if one is not present in DefaultUserName.
4. Specify a default password in DefaultPassword.
   If the DefaultPassword key is not present, click **Edit** > **Add Value**, then specify DefaultPassword as the value name, REG_SZ as the data type, and your default password as the string.
5. Specify 1 as the string for AutoAdminLogon.
   If AutoAdminLogon is not present, add it (AutoAdminLogon as the value name, REG_SZ as the data type, and 1 as the string).
6. Run the demo policy on the agent.
7. Verify that Autologon is enabled is reported.

To protect your computers

- Set the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Winlogon\AutoAdminLogon to 0 and remove delete any DefaultPassword string that may exist.

Inactive accounts

This security check reports accounts that have never logged on to the system and accounts that have not logged on for a specified number of days.

You can monitor the progress of the check by reviewing the query information during the run.

Inactive accounts can be easy targets for intruders. In the Days since last login field, type the number of days allowed by your security policy. The default value is 30.

Use the name lists in the check to exclude users or security groups.

The check returns the following messages:

Message name	Title	Type	Class
Windows 2000: W2KLASTLOG	Inactive account	C	1
Windows NT: LASTLOGTIME	Inactive account	C	1
CHECK_NOT_ PERFORMED	Warning--check could not be performed		1

The Inactive account message can be used to disable reported accounts. See “Correcting agents in messages” on page 42.

To demonstrate the check

1. Create a test account.
2. In a demo policy, disable all checks in the Login Parameters module except Inactive accounts.
3. Run the demo policy on the agent.
4. Verify that Inactive account is reported.
   If Warning—check could not be performed is reported, the LAN Manager Server service is not running. Start the service and rerun the policy.

To protect your computers

◆ Use the Correct function in the console grid to disable unauthorized accounts.

Inactive account timeout (Windows 2000/XP/Server 2003)

Use this option to specify the maximum number of minutes for the Inactive accounts check. The default value is 1200 minutes (20 hours).

Network Integrity

The Network Integrity module reports the vulnerabilities of domains, including global security groups and folder and printer shares. The module also reports CD-ROM and floppy disk drives that can be accessed by network users, and it evaluates Microsoft's Routing and Remote Access Service (RRAS), which is called Remote Access Service (RAS) on Windows NT.

Warning: Improperly editing the Windows registry can cause serious, system-wide problems. Update the Windows Emergency Repair disk before making any changes.

Many Network Integrity checks are correctable and/or updateable. See "Correcting agents in messages" on page 42 and "Updating template and snapshot files in messages" on page 42.

Trusted domains (Windows NT/2000)

This security check for domain controllers reports trusted domains.

Trusted domains provide additional points of access to the system. If security controls are not in place, pass-through authentication can give users unauthorized access to critical files and directories on the system.

The check returns the following message:

Message name	Title	Class
TRUSTED_DOMAINS	Trusted domains	0

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Trusted domains.
2. Ensure that the agent has at least one trusted domain.
3. Run the demo policy on the agent.
4. Verify that Trusted domains is reported.

To protect your computers

- Ensure that reported domains contain only authorized user accounts.

Local groups

This security check reports the agent's local security groups.

All members of a local security group have all rights that are assigned to the group. Because local security groups can have both user accounts and global security groups, some rights may not be appropriate to all members.

The check returns the following message:

Message name	Title	Class
LOCAL_GROUP	Local groups	0

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Local groups.
2. Click **Start** > **Control Panel** > **Administrative Tools** > **Computer Management**, then create one or more local groups.
3. Run the demo policy on the agent.
4. Verify that all local groups are reported.

To protect your computers

- ◆ Ensure that all rights that are assigned to the members of each group are authorized reported domains.

  Windows 2000: Ensure that NTFS permissions on shared directories are set appropriately. They protect shared directories from malicious acts even when share permissions are not set appropriately because Windows 2000 applies the more restrictive of the permissions.

Shared folders

This security check reports folders that are shared with other systems.

If shared folders are in a FAT partition, the permission shares are your protection against intruders.

If the folders are in an NTFS partition, Windows considers both the share permissions and the NTFS file and folders permissions, then applies the more restrictive permissions.

Shared folders are system entry points. Intruders can use them to transfer malicious executable objects to the system.

The check returns the following messages:

Message name	Title	Class
SHARED_DIRECTORIES	Shared folders	0
CHECK_NOT_PERFORMED	Warning - check could not be performed	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Shared folders.
2. Run the demo policy on the agent.
3. Verify that all shared folders are reported.
   When the LAN Manager Server service is not running, the check cannot be performed. Start the service, then rerun the demo policy.

To protect your computers

- Share system folders only with members of the Administrators security group.

Shared folders giving all users Full Control

This security check reports shared folders that grant Full Control to the Everyone security group.

Windows assigns permissions through the Everyone group to maintain backward compatibility with applications that require Read access for Anonymous users. These applications access some file system and registry objects.

Only shares that have been specifically authorized should give all users Full Control.

Administrators can control the membership of all default local groups in Windows.

The check returns the following messages:

Message name	Title	Type	Class
SHARED_DIRS_WITH_ALL_ACCESS	Shared folders grant Full Control to Everyone	C	1
CHECK_NOT_PERFORMED	Warning--check could not be performed		1

To demonstrate the check

1. In Windows Explorer or My Computer, grant Full Control permissions to a folder.
2. In a demo policy, disable all checks in the Network Integrity module except Shared folders giving all users Full Control.
3. Run the demo policy on the agent.
4. Verify that Shared folders grant Full Control to Everyone is reported.

   When the LAN Manager Server service is not running, the check cannot be performed. Start the service, then rerun the demo policy.

To protect your computers

- In the console grid, use the Correct feature to remove Everyone share permissions. If Everyone is the only user on the share, add another user before using the Correct feature.

Shared printers

This security check reports the printers that are shared with other systems.

Unauthorized users with access to a shared printer can reroute sensitive documents to a printer in a less secure area.

The check returns the following message:

Message name	Title	Class
SHARED_PRINTERS	Shared printers	0

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Shared printers.
2. Run the demo policy on the agent.
3. Verify that all shared printers are reported.

   Windows NT: The check cannot be performed when the LAN Manager Server service is not running. Start the service, then rerun the demo policy.

To protect your systems

- Restrict printer access to authorized users.

Share permissions

This security check reports permissions on all shared directories and printers.

FAT partitions: permissions on shared folders are your protection.

NTFS partitions: Windows considers both share permissions and NTFS file and directory permissions, then applies the more restrictive permissions.

Shared directories and printers are defined points of entry to the system. If appropriate permissions are not set, intruders can use them to transfer malicious executable objects to the system or divert critical documents to less secure printers.

The check returns the following message:

Message name	Title	Class
ACCOUNT_SHARE_PERMISSIONS	Share permissions	0

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Share permissions.
2. Run the demo policy on the agent.
3. Verify that Share permissions is reported on all shared folders.

   Windows NT: The check cannot be performed when the LAN Manager Server service is not running. Start the service, then rerun the demo policy.

To protect your computers

- Ensure that permissions are set appropriately.

  Windows 2000: Ensure that the NTFS permissions on shared directories are set appropriately. NTFS permissions protect shared directories from malicious acts, even if the share permissions are not set appropriately, because Windows 2000 applies the more restrictive permissions.

Hidden shares

This security check reports hidden shares on the system.

If intruders discover any hidden shares, they can use them to access the system.

The check returns the following messages:

Message name	Title	Class
HIDDEN_SHARES	Hidden shares	0
CHECK_NOT_ PERFORMED	Warning--check could not be performed	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Hidden shares.
2. Create a hidden share.
3. Ensure that the LAN Manager Server service is running.
4. Run the demo policy.
5. Verify that Hidden shares is reported.

To protect your computers

◆ Delete any hidden shares that are not currently needed.

Anonymous LanMan access disabled

This security check reports a problem if the Anonymous user has access to LAN Manager information such as user names and shares.

The Anonymous user has all rights of the Everyone security group. If access to LAN Manager information is granted to the Anonymous user, remote users can access information about shares and accounts (including the name of a renamed Administrator account).

Warning: Disabling Anonymous access to LAN Manager information can prevent legitimate information gathering by some remote configuration tools.

The check returns the following message:

Message name	Title	Type	Class
ANONYMOUS_LANMAN	Anonymous LAN Manager information access enabled	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Anonymous LanMan access disabled.
2. Run the demo policy on the agent.
3. Verify that Anonymous LAN Manager information access enabled is reported.

To protect your computers

- Use the Correct feature in the console guide to deny Anonymous users access to LAN Manager information by changing the value of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lsa\ restrictanonymous: REG_DWORD: from 0x0 to 0x1.

Permitted TCP ports

This security check reports IP protocol numbers that are permitted by the system.

Use the string list to specify which protocol numbers you want to check. To specify a range of protocol numbers, use a hyphen. For example, for protocols 100 through 255, enter 100-255. Valid protocol numbers are 1-255. The <SYSTEMROOT>\system32\drivers\etc\protocol file includes mappings of protocol names to protocol numbers.

The check returns the following message:

Message name	Title	Class
ALLOWED_PORT_OR_PROTOCOL	The listed port or protocol is permitted by this system	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Permitted TCP ports.
2. Run the demo policy on the agent.

3 Verify that The listed port or protocol is permitted by this system is reported.

To protect your computers

- Filter out unneeded ports.

Permitted UDP ports

This security check reports UDP ports that are permitted to receive incoming connections through the Windows TCP/IP Security settings.

Use the string list to specify which ports you want to examine. To specify a range of ports, use a hyphen. For example, to examine ports 100 through 5000, enter 100-5000. Valid port numbers are 1-65535.

The check returns the following message:

Message name	Title	Class
ALLOWED_PORT_OR_PROTOCOL	The listed port or protocol is permitted by this system	1

To demonstrate the check

1 In a demo policy, disable all checks in the Network Integrity module except Permitted UDP ports.

2 Run the demo policy on the agent.

3 Verify that The listed port or protocol is permitted by this system is reported.

To protect your computers

- Filter out unneeded ports.

Permitted IP protocols

This security check reports IP Protocol numbers that are permitted by the system.

Use the string list to specify which protocol numbers you want to check. You can specify a range of protocol numbers using a hyphen. For example, if you want to check protocol numbers 100 through 255, enter 100-255 in the string list. Valid protocol numbers are 1-255.

The file <SYSTEMROOT>\system32\drivers\etc\protocol contains a mapping of protocol names to protocol numbers.

The check returns the following message:

Message name	Title	Class
ALLOWED_PORT_OR_PROTOCOL	The listed port or protocol is permitted by this system	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Permitted IP protocols.
2. Run the demo policy on the agent.
3. Verify that The listed port or protocol is permitted by this system is reported.

To protect your computers

- Filter out unneeded protocols.

Plain text authentication

This security check reports a problem when plain text authentication is enabled.

If plain text authentication is enabled, anyone monitoring the network can capture and use plain text passwords. However, some third-party resources require plain text authentication.

The check returns the following message:

Message name	Title	Type	Class
PLAIN_TEXT_ENABLED	Plain text authentication is enabled	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Plain text authentication.
2. Run Regedt32.exe and go to HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters.
   In the right panel, the enableplaintextpassword: REG_DWORD: value should be 0 or blank.
3. Double-click **enableplaintextpassword: REG_DWORD:**
4. In the DWORD Editor, change the Data field value to 1.
5. Click **OK**.
6. Run the demo policy on the agent.
7. Verify that Plain text authentication is enabled is reported.

To protect your computers

- Use the Correct feature in the Updateable/Correctable field of the console grid to disable plain text authentication on reported computers.

File security more restrictive than share security

This security check reports a problem when share permissions are more restrictive than file permissions.

Use the name lists to enable or disable the keys that determine whether the check examines the entire directory tree for each share or only for files.

Shared folders are defined points of entry to the system. If appropriate permissions are not set, intruders can use them to transfer malicious executable objects to the system.

The check returns the following messages:

Message name	Title	Class
SHARE_FILE_ PERMISSIONS	Share permissions are more restrictive than file permissions	1
CHECK_NOT_PERFORMED	Warning - check could not be performed	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except File security more restrictive than share security.
2. Enable the Check Files key in the name list.

3 In a test directory on an NTFS volume, right-click a test file, then click **Properties** > **Security** > **Permissions**.

4 Grant the Everyone group Full Control access to the file.

5 Right-click the test directory, then click **Properties**.

6 Click **Sharing** > **Share as** > **Permissions**.

7 Grant the right, Change access to the directory, to the Everyone group.

8 Run the demo policy on the agent.

9 Verify that Share permissions are more restrictive than file permissions is reported.
The check cannot be performed when the LAN Manager Server service is not running. Start the service, then rerun the demo policy.

To protect your computers

◆ Ensure the reported file and share permissions are set properly. Although Windows applies the more restrictive permissions, file permissions should at least match the protection levels provided by the share permissions.

RRAS enabled (Windows 2000/XP)

This security check reports a problem when Routing and Remote Access Service (RRAS) is enabled on the system.

If RRAS is enabled, remote users can access the system and the potential exists for unauthorized use.

The check returns the following message:

Message name	Title	Class
RRAS_ENABLED	RRAS is enabled	1

To demonstrate the check

1 Select a system that has RRAS enabled.

2 In a demo policy, disable all checks in the Network Integrity module except RRAS enabled.

3 Run the demo policy on the agent.

4 Verify that RRAS is enabled is reported.

To protect your computers

◆ Enable RRAS on systems only when it is absolutely necessary.

RAS enabled (Windows NT)

This security check reports a problem when Remote Access Service (RAS) is enabled on the system.

If RAS is enabled, remote users can access the system. Intruders may exploit this vulnerability.

The check returns the following message:

Message name	Title	Class
RAS_ENABLED	RAS is enabled	1

To demonstrate the check

1. Select a system that has RAS enabled.
2. In a demo policy, disable all checks in the Network Integrity module except RAS enabled.
3. Run the demo policy on the agent.
4. Verify that RAS is enabled is reported.

To protect your computers

◆ Enable RAS on systems only when it is absolutely necessary.

RAS installed (Windows NT)

This security check reports a problem when Remote Access Service (RAS) is installed.

If RAS is installed, the potential exists for someone to enable it. With RAS enabled, remote users can access the system. The potential exists for unauthorized use.

The check returns the following message:

Message name	Title	Class
RAS_INSTALLED	RAS is installed	1

To demonstrate the check

1. Select a system that has RAS installed.
2. In a demo policy, disable all checks in the Network Integrity module except RAS installed.

3. Run the demonstration policy on the agent.
4. Verify that RAS is installed is reported.

To protect your computers

- Install RAS on systems only when it is absolutely necessary.

RRAS requires account callbacks (Windows 2000/XP)

This security check reports a problem when RRAS does not require a callback on all accounts.

Enabling RRAS requires users to provide the telephone number that they are calling from to establish a connection. The system can log these telephone numbers for review and follow-up action by a system administrator.

The check returns the following message:

Message name	Title	Class
RRAS_CALLBACK_USER_DISABLED	RRAS callback set by user is disabled	1

To demonstrate the check

1. Select a system that has RRAS enabled.
2. In a demo policy, disable all checks in the Network Integrity module except RRAS requires account callbacks.
3. In the Windows Control Panel click **Administrative Tools** > **Remote Access Server** > **Users** > **Permissions.**
4. Select a user.
5. Click **Grant dialin permission to user** or **Grant all**.
6. Set the Call back option to No Call Back.
7. Run the demo policy on the agent.
8. Verify that RRAS callback set by user is disabled is reported.

To protect your computers

- Enable the Set By Caller option as a minimum.

RAS requires account callbacks (Windows NT)

This security check reports a problem when RAS does not require a callback on all accounts.

Enabling RAS requires users to provide the telephone number that they are calling from to establish a connection. The system can log these telephone numbers for review and follow-up action by a system administrator.

The check returns the following message:

Message name	Title	Class
RAS_CALLBACK_USER_DISABLED	RAS callback set by user is disabled	1

To demonstrate the check

1. Select a system that has RAS enabled.
2. In a demo policy, disable all checks in the Network Integrity module except RAS requires account callbacks.
3. In the Windows Control Panel click **Administrative Tools** > **Remote Access Server** > **Users** > **Permissions.**
4. Click a user.
5. Click either **Grant dialin permission to user** or **Grant all**.
6. Set the Call back option to No Call Back.
7. Run the demo policy on the agent.
8. Verify that RAS callback set by user is disabled is reported.

To protect your computers

◆ Enable the Set By Caller option as a minimum.

RRAS requires preset number for callback (Windows 2000/XP)

This security check reports a problem when RRAS does not require a preset number on all accounts that are required to use callback.

This feature provides the most security for RRAS dial-in control. Intruders must physically access a known telephone number before they can establish a connection.

The check returns the following message:

Message name	Title	Class
RRAS_CALLBACK_PRESET_DISABLED	RRAS callback preset is disabled	1

To demonstrate the check

1. Select a system that has RRAS enabled.
2. In a demo policy, disable all checks in the Network Integrity module except RRAS requires preset number for callback.
3. Click **Network and Dial-up Connections** > **Advanced** > **Dial-up Preferences** > **Ask me during dialing when the server offers**.
4. Run the demo policy on the agent.
5. Verify that RRAS callback preset is disabled is reported.

To protect your computers

◆ Enable this feature for users who always connect using a preset number.

RAS requires preset number for callback (Windows NT)

This security check reports a problem when RAS does not require a preset number on all accounts that are required to use callback.

This feature provides the most security for RAS dial-in control. Intruders must physically access a known telephone number before they can establish a connection.

The check returns the following message:

Message name	Title	Class
RAS_CALLBACK_PRESET_DISABLED	RAS callback preset is disabled	1

To demonstrate the check

1. Select a system that has RAS enabled.
2. In a demo policy, disable all checks in the Network Integrity module except RAS requires preset number for callback.
3. Click **Network and Dial-up Connections** > **Advanced** > **Dial-up Preferences** > **Ask me during dialing when the server offers**.
4. Run the demo policy on the agent.
5. Verify that RAS callback preset is disabled is reported.

To protect your computers

◆ Enable this feature for users who always connect using a preset number.

RRAS NetBIOS gateway disabled (Windows 2000/XP)

This security check reports a problem if the NetBIOS gateway is enabled.

Disabling the NetBIOS gateway limits users to the RRAS server's local resources and prohibits access to network resources.

The check returns the following message:

Message name	Title	Class
RRAS_NETBIOS_ENABLED	RRAS NetBIOS gateway is enabled	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except RRAS NetBIOS gateway disabled.
2. Run Regedt32.exe and access the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ RemoteAccess\Parameters\Ip key in the Windows registry.
3. Ensure that one of the values for this key is AllowNetworkAccess: REG_DWORD:0X1.

   REG_DWORD:0X0 value is 0 or missing, NetBios gateway is disabled. If the REG_DWORD:0X1 value is one, NetBios gateway is enabled.
4. Run the demo policy on the agent.
5. Verify that RRAS NetBIOS gateway is enabled is reported.

To protect your computers

◆ Disable the RRAS NetBIOS gateway.

RAS NetBIOS gateway disabled (Windows NT)

This security check verifies that the NetBIOS gateway is disabled.

Disabling the NetBIOS gateway limits users to the RAS server's local resources and prohibits access to network resources.

The check returns the following message:

Message name	Title	Class
RAS_NETBIOS_ENABLED	RAS NetBIOS gateway is enabled	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except RAS NetBIOS Gateway Disabled.
2. Run Regedt32.exe and access the HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\ RemoteAccess\Parameters\Ip key in the Windows registry.
3. Ensure that one of the values for this key is AllowNetworkAccess: REG_DWORD:0X1.
   REG_DWORD:0X0 value is 0 or missing, NetBios gateway is disabled. If the REG_DWORD:0X1 value is one, NetBios gateway is enabled.
4. Run the demo policy on the agent.
5. Verify that RAS NetBIOS gateway is enabled is reported.

To protect your computers

- Disable the RAS NetBIOS gateway.

RAS encrypted password (Windows NT)

This check reports a problem if the RAS server does not use the Crypto-Handshake Authentication Protocol while authenticating clients.

This authentication protocol ensures that all data transmitted during the session is encrypted.

The check returns the following message:

Message name	Title	Class
RAS_NON_ENCRYPTED_PASSWORD	RAS authentication does not use an encrypted password	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except RAS encrypted password.
2. Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\ CurrentControlSet\Services\ RasMan\PPP key in the Windows registry. Ensure that one of the values for this key is ForceEncryptedPassword: REG_DWORD:0X0.
   If the DWORD value is 0 or missing, ForceEncryptedPassword is disabled. If the DWORD value is 1, ForceEncryptedPassword is enabled.
3. Run the demo policy on the agent.
4. Verify that RAS authentication does not use an encrypted password is reported.

To protect your computers

- Enable Crypto-Handshake Authentication Protocol to authenticate clients.

RAS authentication retries (Windows NT)

This security check reports a problem when the maximum number of unsuccessful RAS authentication retries can exceed the number of Authentication retries that is specified in the check.

The number of RAS authentication retries should not be higher than the number that is specified in your policy. Log on retries should be kept low to discourage brute-force password guessing.

The check returns the following message:

Message name	Title	Class
RAS_AUTH_RETRIES	Too many RAS authentication retries	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except RAS authentication retries.
2. Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\ CurrentControlSet\Services\ RemoteAccess\Parameters key in the Windows registry. Ensure that one of the values for this key is AuthenticateRetries: REG_DWORD:0X0.
   If the DWORD value is 0 or missing, AuthenticateRetries is disabled. If the DWORD value is 1, AuthenticateRetries is enabled.

3 Run the demo policy on the agent.

4 Verify that Too many RAS authentication retries is reported.

To protect your computers

- Set RAS authentication retries to 2.

RAS authentication time limit (Windows NT)

This security check reports when the maximum time limit for RAS authentication can exceed the Time limit (seconds) that is specified in the check.

The maximum time limit for RAS authentication should not be higher than the time limit that is specified in your policy. The time allowance for RAS authentication should be kept low to discourage brute-force logon attacks.

The check returns the following message:

Message name	Title	Class
RAS_AUTH_TIME_LIMIT	RAS authentication time limit too long	1

To demonstrate the check

1 In a demo policy, disable all checks in the Network Integrity module except RAS authentication time limit.

2 Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\ CurrentControlSet\Services\ RemoteAccess\Parameters key in the Windows registry. Ensure that one of the values for this key is AuthenticateRetries: REG_DWORD:0X0.
If the DWORD value is 0 or missing, AuthenticateTime is disabled. If the DWORD value is 1, AuthenticateTime is enabled.

3 Run the demo policy on the agent.

4 Verify that RAS authentication time limit too long is reported.

To protect your computers

- Set the time limit to 120 seconds or less.

RAS NetBIOS auditing (Windows NT)

This security check reports a problem when NetBIOS sessions auditing is not enabled.

If RAS NetBIOS session auditing is disabled, then network activity audits cannot be generated for RAS users.

The check returns the following message:

Message name	Title	Class
RAS_NETBIOS_AUDITING_DISABLED	RAS NetBIOS session auditing is disabled	1

To demonstrate the check

1 In a demo policy, disable all checks in the Network Integrity module except RAS NetBIOS auditing.

2 Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\ CurrentControlSet\Services\ RemoteAccess\Parameters\NetBiosGateway key in the Windows registry. Ensure that one of the values for this key is EnableNetbiosSessionsAuditing: REG_DWORD:0X0.

   EnableNetbiosSessionsAuditing is disabled if the DWORD value is 0 or missing. EnableNetbiosSessionsAuditing is enabled if the DWORD value is 1.

3 Run the demo policy on the agent.

4 Verify that RAS NetBIOS session auditing is disabled is reported.

To protect your computers

◆ Enable session auditing if RAS is running.

RAS auditing (Windows NT)

This security check verifies that RAS auditing is enabled.

If RAS auditing is disabled, then audits will not be generated for RAS users.

The check returns the following message:

Message name	Title	Class
RAS_AUDITING_DISABLED	RAS auditing is disabled	1

To demonstrate the check:

1 In a demo policy, disable all checks in the Network Integrity module except RAS auditing.

2 Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\ CurrentControlSet\Services\ RemoteAccess\Parameters\NetBiosGateway key in the Windows registry. Ensure that one of the values for this key is EnableAudit: REG_DWORD:0X0.

If the DWORD value is 0 or missing, EnableAudit is disabled. EnableAudit is enabled if the DWORD value is 1.

3 Run the demonstration policy on the agent.

4 Verify that RAS auditing is disabled is displayed.

To protect your computers

- Enable RAS auditing if RAS is running.

RAS encrypted data (Windows NT)

This security check verifies that RAS data encryption is enabled.

RAS does not encrypt data transmissions. Unencrypted data transmissions are subject to snoop attacks.

The check returns the following message:

Message name	Title	Class
RAS_NON_ENCRYPTED_DATA	RAS does not encrypt transmitted data	1

To demonstrate the check

1 In a demo policy, disable all checks in the Network Integrity module except RAS encrypted data.

2 Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\ RemoteAccess\Parameters\NetBiosGateway key in the Windows registry. Ensure that one of the values for this key is ForceEncryptedData: REG_DWORD:0X0.
If the DWORD value is 0 or missing, ForceEncryptedData is disabled. ForceEncryptedData is enabled if the DWORD value is 1.

3 Run the demonstration policy on the agent.

4 Verify that RAS does not encrypt transmitted data is reported.

To protect your computers

- Encrypt all data transmissions.

Listening TCP ports

This security check reports listening TCP ports. In the name list, enter the numbers of ports that you want to exclude.

The check returns the following message:

Message name	Title	Class
OPEN_PORT	The named port is listening	4

To demonstrate the check

1. If you have not already done so, run the demo policy to create a snapshot file.
2. Open a new port.
3. In a demo policy, disable all checks in the Network Integrity module except Listening TCP ports.
4. Run the demo policy on the agent.
5. Verify that The named port is listening is reported. The port number is reported in the Name field and the owning process in the Information field.

To protect your computers

- Close unauthorized listening ports.

Listening UDP ports

This check reports listening UDP ports. In the name list, enter the numbers of ports that you want to exclude.

The check returns the following message:

Message name	Title	Class
OPEN_PORT	The named port is listening	4

To demonstrate the check

1. If you have not already done so, run the demo policy to create a snapshot file.
2. Open a new port.
3. In a demo policy, disable all checks in the Network Integrity module except Listening UDP ports.

4 Run the demo policy on the agent.

5 Verify that The named port is listening is reported. The port number is reported in the Name field and the owning process in the Information field.

To protect your computers

- ◆ Close unauthorized listening ports.

New listening TCP ports

This check reports TCP ports that were opened for listening after the last snapshot update.

On agents that use Security Update 12 or lower, this check reports both TCP and UDP ports.

On agents that use Security Update 13 or higher, the check returns the following message:

Message name	Title	Type	Class
NEW_LISTENING_TCP_PORT	New listening TCP port	SU	4

To demonstrate the check

1 If you have not already done so, run the demo policy to create a snapshot.

2 Open a new port.

3 In the demo policy, disable all checks in the Network Integrity module except New listening TCP ports.

4 Run the demo policy on the agent.

5 Verify that New listening TCP port is reported.

To protect your computers

- ◆ Do one of the following:
  - ■ For new authorized listening ports, update the snapshot in the console grid.
  - ■ Close unauthorized listening ports.

Deleted listening TCP ports

This check reports TCP ports that were closed for listening after the last snapshot update.

On agents that use Security Update 12 or lower, the check reports both TCP and UDP ports.

On agents that use Security Update 13 or higher, the check returns the following message:

Message name	Title	Type	Class
DELETED_LISTENING_TCP_PORT	Deleted listening TCP port	SU	3

To demonstrate the check

1. If you have not already done so, run a demo policy with at least one listening TCP port to create a snapshot.
2. Delete a listening TCP port.
3. In the demo policy, disable all checks in the Network Integrity module except Deleted listening TCP ports.
4. Run the demo policy on the agent.
5. Verify that Deleted listening TCP port is reported.

To protect your computers

◆ Do one of the following:

- For authorized deletions, update the snapshot in the console grid.
- Restore listening TCP ports that should not have been deleted.

New network shares

This security check reports network shares were added to the agent after the last snapshot update.

The check returns the following messages:

Message name	Title	Type	Class
NEW_NETWORK_SHARE	New network share	SU	4

To demonstrate the check

1. If you have not already done so, run a demo policy to create a snapshot file.
2. In a demo policy, disable all checks in the Network Integrity module except New network shares.
3. Run the policy on the agent.
4. In Windows Explorer, share a folder that was not previously shared.
5. Run the policy on the agent.
6. Verify that New network share is reported.

To protect your computers

- Do one of the following:
  - For authorized new shares, update the snapshot in the console grid.
  - Remove unauthorized shares.

Modified network shares

This security check reports network share changes if the path or share type has changed on the agent since the last snapshot update.

The check returns the following message:

Message name	Title	Type	Class
MODIFIED_NETWORK_SHARE	Modified network share	SU	3

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except Modified network shares.
2. Add a share.
3. If you have not already done so, run the Network Integrity module on the agent computer to create the snapshot file.
4. Remove the share.
5. Share a different folder that uses the same share name as the one you removed in step 4.
6. Run the demo policy on the agent.
7. Verify that Modified network share is reported.

To protect your computers

- Do one of the following:
  - For authorized share changes, update the snapshot in the console grid.
  - For unauthorized share changes, restore the shares from a backup.

Deleted network shares

This security check reports deleted network shares that were deleted from the agent after the last snapshot update.

The check returns the following updateable messages:

Message name	Title	Type	Class
DELETED_NETWORK_SHARE	Deleted network share	SU	3

To demonstrate the check

1. If you have not already done so, run a demo policy to create a snapshot.
2. In the demo policy, disable all checks in the Network Integrity module except Deleted network shares.
3. In Windows Explorer, remove a share.
4. Run the demo policy on the agent.
5. Verify that Deleted network share is reported.

To protect your computers

- Do one of the following:
  - For authorized deletions, update the snapshot in the console grid.
  - Restore shares that should not have been deleted.

LanMan authentication (Windows NT)

This security check reports a problem when LAN Manager authentication is enabled.

LAN Manager uses a relatively weak form of encryption. Intruders sniffing the network may be able to capture and crack the password hash.

The check returns the following message:

Message name	Title	Class
LANMAN_ENABLED	Lanman authentication is enabled	1

To demonstrate the check

1. In a demo policy, disable all checks in the Network Integrity module except LanMan authentication.
2. Run Regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\Lsa key in the Windows registry. One of the values on the right side of the display should be Lmcompatibilitylevel: REG_DWORD:0X2.
   If the DWORD value is 0 or missing, Windows NT sends LAN Manager and Windows NT authentication to the server. If the DWORD value is 1, Windows NT sends LAN Manager authentication only if requested by the server. If the DWORD value is 2, Windows NT never sends LAN Manager authentication.
3. If the DWORD value is 2, click the Lmcompatibilitylevel value.
   On the menu bar, click **Edit**, then click **Delete**.
4. Run the demonstration policy on the agent.
5. Verify that Lanman authentication is enabled is reported.

To protect your computers

◆ Disable LAN Manager authentication.

New listening UDP ports

This check reports UDP ports were opened for listening after the last snapshot update.

On agents that use Security Update 12 or lower, the check reports no messages. Use the New listening TCP ports check, which reports both TCP and UDP ports.

On agents that use Security Update 13 or higher, the check returns the following message:

Message name	Title	Type	Class
NEW_LISTENING_UDP_PORT	New listening UDP port	SU	4

To demonstrate the check

1. If you have not already done so, run the demo policy to create a snapshot.
2. Open a new port.
3. In the demo policy, disable all checks in the Network Integrity module except New listening UDP ports.

4 Run the demo policy on the agent.

5 Verify that New listening UDP port is reported.

To protect your computers

◆ Do one of the following:

- For new authorized listening ports, update the snapshot in the console grid.
- Close unauthorized listening ports.

Deleted listening UDP ports

This check reports UDP ports that were closed for listening after the last snapshot update.

On agents that use Security Update 12 or lower, the check reports no messages. Use Deleted listening TCP ports, which reports both TCP and UDP ports.

On agents that use Security Update 13 or higher, the check returns the following message:

Message name	Title	Type	Class
DELETED_LISTENING_UDP_PORT	Deleted listening UDP port	SU	3

To demonstrate the check

1 If you have not already done so, run a demo policy with at least one listening UDP port to create a snapshot.

2 Delete a listening UDP port.

3 In the demo policy, disable all checks in the Network Integrity module except Deleted listening UDP ports.

4 Run the demo policy on the agent.

5 Verify that Deleted listening UDP port is reported.

To protect your computers

◆ Do one of the following:

- For authorized deletions, update the snapshot in the console grid.
- Restore listening UDP ports that should not have been deleted.

Object Integrity

Security checks in the Object Integrity module examine ACL support for changes in ownership, permissions, the logical-name table, rights identifiers, and other software objects or device-specific files in the system device directory. The module also detects new devices, deleted devices, and device changes between policy runs.

Volumes without ACL control

This security check reports volumes that do not support persistent ACLs.

You can use the name list to exclude volume names such as MYDISK, file systems such as HPFS, or root folders such as C:\ from the check.

These volumes are inherently insecure because they allow anyone to add, modify, or delete files and directories.

The check returns the following message:

Message name	Title	Class
NOACL	Volume with file system that does not support ACLs	1

To demonstrate the check

1. Select a system that has a non-NTFS volume.
2. In a demo policy, disable all checks in the Object Integrity module except Volumes without ACL control.
3. Run the demo policy on the agent.
4. Verify that Volume with file system that does not support ACLs is reported.

To protect your computers

- Do one of the following:
  - Convert the reported volumes to NTFS.
  - Set the appropriate access security on the files and directories.

Local accounts

This security check reports all local accounts.

You can use the check's name list to exclude accounts such as guest and administrator.

Accounts that are created on a domain controller are all domain accounts. This check is for workstations and Professional systems.

Because global security groups can become members of local security groups, the need for additional local accounts should be minimal.

The check returns the following messages:

Message name	Title	Class
NOLOCAL	User or group defined on local system	1

To demonstrate the check

1. Select a system that has a local account.
2. In a demo policy, disable all checks in the Object Integrity module except Local accounts.
3. Run the demo policy on the agent.
4. Verify that User or group defined on local system message is reported.
   The check cannot be performed when the LAN Manager Server service is not running. Start the service, then rerun the demo policy.

To protect your computers

- Delete local accounts when they are no longer needed.

OS Patches

The OS Patches module reports patches that have been released for Windows by Microsoft Corporation but are not found on the agent. Released patches are defined in template files. New patch templates are available every two weeks through LiveUpdate.

Application patches

Patches for Microsoft Internet Explorer and Microsoft Outlook are included in Patch templates. Patches for Microsoft Internet Information Server are included in Application Patch templates (iis.ps4 and iis.ps5).

Editing the Patch template

The Patch template defines patches that are to be examined by the module.

You can add or delete Patch templates. You can also copy and rename Patch template files, then add checks for operating system patches and hot fixes that are not yet identified by default templates.

Warning: Symantec ESM baseline policies and best practice policies do not behave properly if you modify default templates patch.pw4, patch.ps4, patch.pw5, patch.ps5, patch.pwx, or patch.p6s.

To add a new Patch template

1. In the enterprise tree, right-click the Templates node, then click **New**.
2. In the Available template types list, click one of the following options to specify the type of template that you want to add:
   - **Patch - NT Server 4.0**
   - **Patch - NT Workstation 4.0**
   - **Patch - Windows 2000 Professional**
   - **Patch - Windows 2000 Server**
   - **Patch - Windows XP Professional**
   - **Patch - Windows Server 2003**
3. In the Template file name text box, type a new template name of no more than eight characters, without a file extension. The appropriate file extension is automatically added, depending on the template type that is selected in step 2.
4. Press **Enter**.

To copy and rename a Patch template

1. In Windows Explorer, open the \ESM\template directory on the manager that contains the template file that you want to edit.
2. Copy the template file that you want to edit in the \ESM\template directory.
3. Rename the copy. The file name must not exceed eight characters. Do not change the file extension.
4. Exit Windows Explorer.

To add a record to a Patch template

1. Create a copy of the Patch template that you want to use, and edit it, not the original template.
2. In the enterprise tree, double-click the template that you want to edit.
3. Click **Add Row**.
4. In the following fields of the new row, replace <NEW> with the corresponding information.

Field	Information
CERT ID	ID number assigned to a CERT advisory or vendor's bulletin (e.g. CERT CA-2001-13, Microsoft: MS01-033)
Date	Date that an advisory or bulletin was published or last updated in the yyyy/mm/dd format
OS	Operating system
OSVer/SPVer	Operating system version and one or more service pack levels (e.g. 5.0-SP0, SP1, SP2)
Patch ID	Enter one of the following: ■ NT: SERVICE PACK # (current Service Pack is 6) ■ PENDING ■ ID that starts with Q, q, KB, or kb for registry checks ■ ID that starts with F or f for file-only checks
Architecture	Currently not used in Windows Patch templates
Description	Patch description (usually matches advisory or bulletin title)

5 In the Severity field, replace <NEW> with a code that identifies which message will be reported to identify missing or forbidden patches:

Severity	Message name	Security level
0	PATCHNOTINS0	Green
1	PATCHNOTINS1	Yellow
2	PATCHNOTINS2	Yellow
3	PATCHNOTINS3	Red
0	FORBIDDEN_PATCH_0	Green
1	FORBIDDEN_PATCH_1	Yellow
2	FORBIDDEN_PATCH_2	Yellow

If the Patch ID value is PENDING, a severity code of 2 or 3 is required. In this case, the severity code determines whether the security message will be red or yellow when a patch is available.

Severity	Message name	Security level
2	PATCHNOTAVAIL2	Yellow
3	PATCHNOTAVAIL3	Red

A severity code greater than 3 defaults to PATCHNOTINS3 or PATCHNOTAVAIL3.

6 Click the Type field, then select one of the following:

- **Mandatory** This patch must be installed.
- **Forbidden** This patch must not be installed.
- **Optional** This is a rollup patch that is not required, but supersedes other patches listed in the template. If this patch is not installed, no message is reported for this patch.

7 Add rows to the following sublists:

- File (see "To add a row to the Files sublist" on page 196).
- Superseded (see "To add a row to the Superseded sublist" on page 196).
- Conditions (see "To add a row to the Conditions sublist" on page 196).

8 Click **Save**.
To add another row, repeat steps 2–7.

9 Click **OK** to exit the Template Editor.

To add a row to the Files sublist

1 If the Template Editor is not already open, in the enterprise tree, double-click the Patch template that you want to edit.

2 In the row that you want to edit, click the File field (initially 0).

3 In the Template Sublist Editor, click **Add Row.**

4 In the File field of the new row, replace <NEW> with the absolute path of the patch file.

Path names can include variable keywords that represent data in Windows registry values. Keywords must be defined in the Patch Keywords template before they are used in the Patch template. See “Editing the Patch Keywords template” on page 198.

5 In the Date/Version field, replace <NEW> with the date of the file in yyyy/mm/dd format or the character v followed by a version string.

The Patch module looks for dates and versions that are equal to or greater than the dates and versions that are specified to determine whether a patch has been installed.

6 Click **Apply**.

To add another row, repeat steps 2–6.

7 Click **Close** to exit the Template Sublist Editor.

To add a row to the Superseded sublist

1 If the Template Editor is not already open, in the enterprise tree, double-click the Patch template that you want to edit.

2 In the row that you want to edit, click the Superseded field (initially 0).

3 In the Template Sublist Editor, click **Add Row.**

4 Click the Description field, then select **Replaced by** or **Replaces**.

5 In the Patch ID field, replace <NEW> with the ID number of the new patch or old patch.

6 Click **Apply**.

To add another row, repeat steps 2–5

7 Click **Close** to exit the Template Sublist Editor.

To add a row to the Conditions sublist

1 In the enterprise tree, double-click the Patch template that you want to edit.

2 In the Template Editor, click the Conditions field of the row that you are editing.

3 Click **Add Row**.

4 In the Template Sublist Editor, click the Type field, then select one the following conditions:

- **Running** Look for the patch only if the service is running.
- **Installed** Look for the patch if the service is installed.
- **File** Look for the patch if the listed file exists.
- **Registry** Look for the patch if the listed registry key exists.
- **Registry Value** Look for the patch if the reported registry value exists and satisfies the equation.
- **Registry Key Default Value** Look for the patch if the listed registry key's default value exists and satisfies the equation.

Note: Beginning with SU 13, Registry Value and Registry Key Default Value can be verified for applications. See "Application patches" on page 193. It is not necessary to edit the equation that identifies registry values to use these options.

Add a valid comparison operator to the end of the registry key followed by the value in double quotes. For example: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet explorer\Version Vector\IE="6.0000"

5 Click the Name field, then replace <NEW> with the name of a service that must be enabled or a process that must be running before the patch is examined.

Type service names exactly as they appear in the Windows Services window. To verify service names, click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

6 Click **Apply**.

To add another row, repeat steps 2–5.

7 Click **Close** to exit the Template Sublist Editor.

Comparison operators

Use the following operators for Registry Value or Registry Key Default Value options in the Conditions sublist:

Operator	Value type
=~	Regular expression

Operator	Value type
= =! < > <= >=	String or number

For greater than or less than operators, numbers are greater than letters. For example, “123>abs” is true even though abc has a greater ascii value.

Patch Keywords templates

Use this option to enable or disable Patch Keywords .pkl template files that define variable keywords by their registry key values.

After you define a keyword in a Patch Keywords template, you can use it in a file path name in the Patch template.

Note: You can also use the variable keyword %SystemRoot% in your Patch templates. The Patch module looks at the operating system to resolve the location of %SystemRoot% and other keywords that are used by the operating system.

When a match is not found for text that appears to be a keyword in the Patch template, the Patch module reports Patch not installed with the file path name that could not be resolved.

Editing the Patch Keywords template

Patch Keywords templates define variable keywords by their registry key values.

Note: If you change the default Patch Keywords template (windows.pkl), the behavior of default Patch templates and Symantec ESM best practice policies will not be predictable.

To add a new Patch Keywords template

1. In the enterprise tree, right-click the Templates node, then click **New**.
2. In the Available template types list, click **Patch Keywords-all**.
3. In the Template file name text box, type a new template name of no more than eight characters. A .pkl file extension is automatically added.

4 Press **Enter**.

To copy and rename a Patch Keywords template

1 In Windows Explorer, open the \ESM\template directory on the manager that contains the template file that you want to edit.

2 Copy the template file that you want to edit to the \ESM\template directory.

3 Rename the copy. The file name must not exceed eight characters. Do not change the file extension.

4 Exit Windows Explorer.

To add a record to a Patch Keywords template

1 If the Template Editor is not already open, in the enterprise tree, double-click the Patch Keywords template that you want to edit.

2 In the Template Editor, click **Add Row**.

3 In the Keyword field of the new row, replace <NEW> with the name of the keyword that you want to use as a variable to represent a registry key value.
Keywords begin and end with % percent sign characters. For example, %KeywordName%

4 In the Keyword Value field, replace <NEW> with the full path name for the Windows registry key value that the keyword represents.

5 Click the Keyword Type field, then select Registry. Other keyword types will be added to this list in future Security Update releases.

6 Click **Save**.
To add another record, repeat steps 2–6.

7 Click **OK**.

Common Patch module messages

The OS Patches (Patch) module reports agents that are not running the operating system patches that are defined in Patch templates. Use the Template file list option to enable or disable template files. The module examines the Patch Keywords template to resolve file path names that are identified by variable keywords in the Patch template.

In addition to the messages reported for specific checks and options, the Patch module also reports the following messages.

Message name	Title	Class
NA_PATCH_STATUS	Cannot determine patch status	2
FORBIDDEN_PATCH_3	Forbidden patch found	0
FORBIDDEN_PATCH_2	Forbidden patch found	0
FORBIDDEN_PATCH_1	Forbidden patch found	0
FORBIDDEN_PATCH_0	Forbidden patch found	0
CHECKING_TYPE_UNCLEAR	Incompatible checking modes specified	4
INVALID_REG_VALUE_FORMAT	Incorrect format for registry value condition	4
INVALID_ARCHITECTURE	Invalid architecture	0
INVALID_OSVER	Invalid OS version	0
INVALID_SPVER	Invalid service pack version	0
SERVICE_PACK_NOT_CURRENT	Latest service pack not installed	4
SERVICE_PACK_NOT_CURRENT	Latest Service Pack not installed	4
NO_TEMPLATE_ SPECIFIED	No applicable template files specified	4
NO_COMPARISON_SPECIFIED	No comparison type specified	4
NO_FILE_INFO	No file information available for patch	4
OPTIONAL_PATCH_NO_SUPERSEDE	Optional patch supersedes nothing	2
UNKNOWN_PATCH_ ID	Patch is not a Registry or File only patch	4
PATCHNOTAVAIL2	Patch not available	2
PATCHNOTAVAIL3	Patch not available	4
PATCHNOTINS0	Patch not installed	0

Message name	Title	Class
PATCHNOTINS1	Patch not installed	2
PATCHNOTINS2	Patch not installed	2
PATCHNOTINS3	Patch not installed	4
INVALID_VALUE_OPERATOR	Registry value comparison operator is invalid	4
INVALID_VALUE_OPERATOR	Registry value comparison operator is invalid	4

Patch templates

Use this option to enable or disable the Patch template files. The module uses only enabled template files that apply to the host. For example, .pwx template files are only used on agents running Windows XP Professional:

Windows operating system	File extension
Server 2003	.p6s
2000 Server	.ps5
2000 Professional	.pw5
NT 4.0 Server	.ps4
NT 4.0 Workstation	.pw4

Comparisons

The module reports a problem when a patch that is defined in the template is missing from the agent. It also reports a problem when the registry key, version number, or file date attribute of the agent patch does not match the attribute specified in the Patch template.

Not all patches can be detected by all detection methods. For example, the Registry key option does not detect F (file) patches. Therefore you may want to enable two or more comparison options.

The module first uses the enabled option that most accurately detects patches. File version is the most accurate method, followed by File date, and Registry key.

One or more comparison options must be enabled to use the Relaxed or Strict check. If none are enabled, the following message is returned:

Message name	Title	Class
NO_COMPARISON_SPECIFIED	No comparison type specified	4

File versions

Enable this option to use file versions to determine whether a patch has been installed. File versions are stored in Files sublists of the Patch template. See "To add a row to the Files sublist" on page 196.

The following message is returned:

Message name	Title	Class
BAD_DATE_OR_VER	Invalid date or version value	4

File dates

Enable this option to use file dates to determine whether a patch has been installed. File dates are stored in Files sublists of the Patch template. See "To add a row to the Files sublist" on page 196.

The following message is returned:

Message name	Title	Class
BAD_DATE_OR_VER	Invalid date or version value	4

Registry keys

Enable this option to use registry values to determine if a patch that begins with Q or KB has been installed. F (file) patches are not validated.

The following message is returned:

Message name	Title	Class
NA_PATCH_STATUS	Cannot determine patch status	4

Relaxed

Enable this option to report a problem if none of the enabled comparison options discover an installed patch. The Relaxed and Strict options are mutually exclusive.

The Relaxed and Strict options are mutually exclusive. When both are enabled, the following message is returned:

Message name	Title	Class
CHECKING_TYPE_UNCLEAR	Incompatible checking modes specified	4

Strict

Enable this option to report a problem if one or more enabled comparison options cannot find the patch that is defined in the template.

The Strict and Relaxed options are mutually exclusive. When both are enabled, the following message is returned:

Message name	Title	Class
CHECKING_TYPE_UNCLEAR	Incompatible checking modes specified	4

Superseded

Enable this option to report a patch and its superseding patches if the patch and all of its superseding patches are missing.

The following message is reported:

Message name	Title	Class
SUPERSEDED_PATCH_NOT_INSTALLED	Superseded patch not installed	0

Disable module

The OS Patches module can take a long time to run. To save time, enable this option if you recently ran the module.

Internet advisory resources

You can obtain current counter-measure information for known security vulnerabilities from Symantec Corporation and other security information clearing houses on the Internet:

Organization	URL
Symantec Security Response	http://securityresponse.symantec.com
CERT Coordination Center	http://www.cert.org
Center for Education and Research in Information Assurance and Security (CERIAS)	http://www.cerias.purdue.edu
Computer Incident Advisory Capability (CIAC)	http://ciac.llnl.gov/ciac/
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org
InfoSysSec	http://www.infosyssec.com
Internet/Network Security	http://netsecurity.about.com
Microsoft Corporation	http://www.microsoft.com
NTBugtraq	http://www.ntbugtraq.com
NTSecurity Net	http://www.ntsecurity.net
SecurityFocus	http://www.securityfocus.com
Storm Center	http://www.incidents.org
System Administration, Networking and Security (SANS)	http://www.sans.org/top20.htm

Password Strength

The Password Strength module reports passwords that do not conform to specified format, length, and expiration requirements. It also applies dictionary tests to detect passwords that are easily guessed.

Unlike other modules, which can be used on shared directories, the Password Strength module must be installed on and run from a local drive.

Many Password Strength checks report the correctable (C) message, Guessed user password. When you use the Correct feature in the console grid to correct reported accounts, the accounts are disabled. The message is identified in the description of the checks that use it. Also see “Correcting agents in messages” on page 42.

How to secure your passwords

Secure passwords:

- Have at least eight characters including one or more non-alphabetic characters.
- Do not match an account or host computer name.
- Cannot be found in any dictionary. See "Wordlist files" on page 209

Users to check

Use this option to specify users and security groups that are excluded or included for all security checks in the module. See "Editing name lists" on page 35.

Minimum password length

This security check reports user accounts that:

- Do not require passwords.
- Have passwords with fewer than the specified number of characters.

In the Minimum number of characters text box, type your policy's required password length. The default value is 8.

Blank passwords are a security risk because anyone with the user name can access the account. Passwords with few characters are relatively easy to guess.

The check returns the following messages:

Message name	Title	Class
MIN_PASSWD_LEN_TOO_LOW	Minimum password length too low	1
PASSNOPASS	System allows blank passwords	4

To demonstrate the check's blank password function

1. In a demo policy, disable all checks in the Password Strength module except Minimum password length.
2. In the Minimum number of characters field, type **8**.
3. In the Minimum password length Windows template security policy, change the agent setting to **0**.
4. Run the demo policy on the agent.
5. Verify that System allows blank passwords is reported.

To demonstrate the check’s password length function

1. In a demo policy, disable all checks in the Password Strength module except Minimum password length.
2. In the Minimum number of characters field, type **8**.
3. In the Windows template security policy, change the agent setting to **6**.
4. Run the demo policy on the agent.
5. Verify that Minimum password length too low is reported.

To protect your computers

- Set the minimum password length in the Windows security policy to at least 8 characters.
  Strong user security controls require longer passwords. Your account policy should require passwords that are long enough to make password guessing difficult and short enough for users to remember. See “How to secure your passwords” on page 205.

Accounts without passwords

This security check for domain controllers reports user accounts that do not have passwords.

You can use the name lists to exclude users or security groups that are not already excluded by the Users to check option.

An account without a password can be accessed by anyone who knows the user name.

The check returns the following messages:

Message	Title	Type	Class
DISABLED_PASSNOUSERPASS	No password on disabled account		0
PASSNOUSERPASS	No password	C	4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property.

Inform the account user of the change and how the user can change the temporary password.

- Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password. See "How to secure your passwords" on page 205.

Password = username

This security check reports accounts with matching user names and passwords.

The check is provided for systems with a large number of user accounts. The security check is not as thorough as Password = any username. However, if the Password = any username check takes too much time or consumes too much CPU, you can use the Password = username check on a daily basis and the Password = any username check on the weekends.

Intruders frequently try a combination of user names and passwords in an attempt to break in.

The check returns the following messages:

Message name	Title	Type	Class
DISABLED_GUESSPASS	Guessed user password on disabled account		0
GUESSPASS	Guessed user password	C	4

To protect your computers

◆ Do one of the following:

- Use the Correct feature to disable the reported accounts that are not needed, then delete them.
- Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
- Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

See "How to secure your passwords" on page 205.

Password = any username

This security check reports user accounts with passwords that match any user name in your system password files.

If this check takes too much time or consumes too much CPU to run on a normal workday, you can run the Password = username check on a daily basis and run this check on the weekends.

Intruders frequently substitute user names for passwords in an attempt to break in.

The check returns the following messages:

Message name	Title	Type	Class
DISABLED_GUESSPASS	Guessed user password on disabled account		0
GUESSPASS	Guessed user password	C	4

To protect your computers

- ◆ Do one of the following:
  - ■ Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - ■ Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
  - ■ Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See “How to secure your passwords” on page 205.

Password = wordlist word

This security check tries to match passwords with words in enabled word files and reports user accounts with matches.

Use the name lists to enable or disable word files for the check.

Checking passwords against word lists significantly increases the time required to complete a policy run. You can shorten the run time by specifying the percentage of words to include in each policy run. The default value is 100 percent. If you specify a smaller value, the check starts at the point in the word lists where the previous policy run ended.

The check returns the following messages:

Message name	Title	Type	Class
DISABLED_GUESSPASS	Guessed user password on disabled account		0
GUESSPASS	Guessed user password	C	4
NOWORDFILES	No word files specified		4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
  - Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See "How to secure your passwords" on page 205.

Wordlist files

The Password = wordlist word check compares passwords to words in dictionary word files(*.wrd files). Passwords that match word file words (and variations of those words) can be easily guessed by intruders and are a security threat.

The Password Strength module provides the following word files. The letters D, FR, I, NL, P, and SP are language identifiers for German, French, Italian, Dutch, Portuguese, and Spanish.

Table 6-1 Wordlist files

Category	File	No. of words
First name	firstnam.wrd Fname_D.wrd Fname_FR.wrd Fname_I.wrd Fname_NL.wrd Fname_P.wrd Fname_SP.wrd	651 1602 784 952 724 449 349

Table 6-1 Wordlist files

Category	File	No. of words
Last name	lastnam.wrd	2958
	Lname_D.wrd	3101
	Lname_FR.wrd	3196
	Lname_I.wrd	2848
	Lname_NL.wrd	3005
	Lname_P.wrd	723
	Lname_SP.wrd	3027
Dictionaries	synopsis.wrd	253
	english.wrd	3489
	lenglish.wrd	34886
	Slist_D.wrd	169
	List_D.wrd	2597
	Llist_D.wrd	19319
	Slist_FR.wrd	166
	List_FR.wrd	2517
	Llist_FR.wrd	17893
	Slist_I.wrd	227
	List_I.wrd	2490
	Llist_I.wrd	14814
	Slist_NL.wrd	399
	List_NL.wrd	3038
	Llist_NL.wrd	14232
	Slist_P.wrd	217
	List_P.wrd	2169
	Llist_P.wrd	16950
	Slist_SP.wrd	162
	List_SP.wrd	2424
	Llist_SP.wrd	19580
	yiddish.wrd	639
Computers	computer.wrd	143
	Compu_D.wrd	545
	Compu_FR.wrd	346
	Compu_I.wrd	255
	Compu_NL.wrd	184
	Compu_P.wrd	226
	Compu_SP.wrd	216
	defaults.wrd	465
	nerdnet-defaults.wrd	142
	ntccrack.wrd	16870
	Oracle.wrd	37
	wormlist.wrd	432

Table 6-1 Wordlist files

Category	File	No. of words
Specialty	cartoon.wrd college.wrd disney.wrd hpotter.wrd python.wrd sports.wrd tolkien.wrd trek.wrd	133 819 433 715 3443 247 471 876

To enable a word file

1 In the Disabled Word Files list, select a word file.

2 Click the left arrow.

To disable a word file

1 In the Enabled Word files list, select a word file.

2 Click the right arrow.

To edit a word file

1 Do one of the following:

- Open an existing word file in a text editor. (Windows word list files are located in C:\Program Files\Symantec\ESM\Words.)
- Create a new ASCII plain-text word file in a text editor. Name the new file with a .wrd extension (for example, medical.wrd).

2 Type only one word per line.

3 Save the file in the words folder.

MD4 hashes

When this option is enabled, password cracking checks look for NT (MD4) hashes as well as LAN Manager hashes.

The option significantly increases module run time, but it is needed to crack passwords that do not have LAN Manager hashes.

For example, an account with a password of more than 14 characters does not have a LAN Manager hash, and password cracking checks do not function properly if this option is not enabled.

When this option is used, all checks that attempt to guess passwords return the following message:

Message name	Title	Type	Class
GUESSPASS	Guessed user password	C	4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
  - Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See "How to secure your passwords" on page 205.

Reverse order

When this option is enabled, module checks that guess passwords report accounts with passwords that match the reverse order of user names or entries in enabled word files; e.g., golf in reverse order matches the password, flog.

Note: When you enable this option, you must also enable the Password = username or Password = any username check and the Password = wordlist word check.

Intruders often use common names or words in reverse order as passwords in an attempt to break in.

The module returns the following message:

Message name	Title	Type	Class
GUESSPASS	Guessed user password	C	4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
  - Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See "How to secure your passwords" on page 205.

Double occurrences

This option causes password checks to report accounts with passwords that match doubled versions of user names or entries in enabled word files; e.g., golf doubled matches the password, golfgolf.

Note: When you enable this option, you must also enable the Password = username or Password = any username check and the Password = wordlist word check.

Intruders often use doubled versions of user names or common words as passwords in an attempt to break in.

The check returns the following message:

Message name	Title	Type	Class
GUESSPASS	Guessed user password	C	4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.

  - Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See "How to secure your passwords" on page 205.

Plural forms

This option causes password checks to report accounts with passwords that match plural forms of user names or entries in enabled word files; e.g., golf in plural form matches the password, golfs.

Note: If you enable this option, you must also enable the Password = username or Password = any username check, and the Password = wordlist word check.

Intruders often use plural forms of user names or common words as passwords in an attempt to break in.

The check returns the following message:

Message name	Title	Type	Class
GUESSPASS	Guessed user password	C	4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
  - Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See "How to secure your passwords" on page 205.

Prefix

This option causes password checks to report accounts with passwords that match forms of user names or entries in enabled word files with a prefix; e.g., golf with the prefix pro matches the password, progolf.

Use the name list to specify prefixes for the check.

Note: If you enable this option, you must also enable the Password = username or Password = any username check and the Password = wordlist word check.

Intruders often add prefixes to user names or common words in an attempt to break in.

The check returns the following message:

Message name	Title	Type	Class
GUESSPASS	Guessed user password	C	4

To protect your computers

- Do one of the following:
  - Use the Correct feature to disable the reported accounts that are not needed, then delete them.
  - Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
  - Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

  See “How to secure your passwords” on page 205.

Suffix

This option causes password checks to report accounts with passwords that match forms of user names or entries in enabled word files with a suffix; e.g., golf with the suffix ball matches the password, golfball.

Use the name list to specify suffixes for the check.

Note: If you enable this option, you must also enable the Password = username or Password = any username check and the Password = wordlist word check.

Intruders often add suffixes to user names or common words in an attempt to break in.

The check returns the following message:

Message name	Title	Type	Class
GUESSPASS	Guessed user password	C	4

To protect your computers

◆ Do one of the following:

- Use the Correct feature to disable the reported accounts that are not needed, then delete them.
- Use the Correct feature to disable the reported account. Assign a more secure temporary password to it, then remove the disabled property. Inform the account user of the change and how the user can change the temporary password.
- Assign a more secure temporary password to the account. Inform the account user of the change and how the user can change the temporary password.

See “How to secure your passwords” on page 205.

Password changes

This security check reports accounts where users cannot change their passwords.

Use the name lists in the check to exclude users or security groups that are not already excluded by the Users to check option.

If a user cannot change the account password, unauthorized users may acquire the password and gain long term access to the account.

The check returns the following message:

Message name	Title	Class
CHANGE_PASSWORD	User cannot change password	1

To protect your computers

◆ In the Account's tab of the user Properties dialog box, uncheck **User cannot change password**.

Password must expire

This security check reports user accounts with the Password never expires property enabled.

By default, this check does not report users who cannot change their passwords. If you want the check to report users who cannot change their passwords, type **Yes** in the Incl. unchangeable text box. Use the name lists in the check to exclude specified users and security groups.

When users are not required to change their account passwords, unauthorized users may acquire the passwords and gain long term access to the system.

The check returns the following messages:

Message name	Title	Class
ACCTPOLICY_PASSWORDS_EXPIRE	Passwords do not expire on system	1
PASSWORDS_EXPIRE	User password never expires	1

To protect your computers

◆ In the Properties dialog box, uncheck **Password never expires.**

Maximum password age

This check reports a problem if the Windows password policy has a maximum password age that exceeds the number of days that is specified in your security policy.

In the Days until expiration text box, type the maximum number of days that your policy allows before a password must be changed.

The longer the period, the more time intruders have to guess the password.

The check returns the following message:

Message name	Title	Class
MAX_PASSWD_AGE_TOO_HIGH	Maximum password age too high	1

To protect your computers

- Set the maximum password age to 60 days or less.

Minimum password age

This security check reports a Windows password policy has a minimum password age that is less than the number of days that is specified in your security policy.

If the minimum password age is too low, users will be tempted to write down passwords because they have difficulty remembering them.

In the Days until change is allowed text box, type the minimum number of days that your policy requires before a password can be changed. The value of 0 (zero) is not valid.

The check returns the following message:

Message name	Title	Class
MIN_PASSWD_AGE_TOO_LOW	Minimum password age too low	1
CHECK_NOT_ PERFORMED	Warning – check could not be performed	1

To protect your computers

- Set the minimum password age to at least 14 days.

Password uniqueness

This security check reports a problem when the account policy in the User Manager for domains does not keep a password history or retains fewer than the required number of passwords.

If users can quickly cycle through the password history to return to their favorite passwords, the purpose of regular changes is defeated.

In the Number of passwords to remember text box, type the number of passwords that should be retained as password history before passwords can be reused.

The check returns the following message:

Message name	Title	Class
MIN_PASSWD_HIST_TOO_LOW	Minimum password history too low	1

To protect your computers

◆ Set the minimum password history to at least 10.

Syskey encryption

This security check reports a problem when the Security Account Manager (SAM) does not enable Syskey encryption. Windows NT requires Service Pack 3.

Encrypted passwords are more secure when the SAM that stores passwords applies this additional encryption.

Warning: After you enable Syskey encryption, you cannot disable it.

The check returns the following message:

Message name	Title	Class
SYSKEY_NOT_ENABLED	Passwords not encrypted with syskey	1

To protect your computers

1. Run syskey.exe
2. Select Encryption Enabled.

Registry

Security checks in the Registry module compare current settings with Registry template records and report changes in registry key ownership, registry keys and values, and last write times of registry keys.

Some module messages can be used to update snapshots to match current agent settings. See "Updating template and snapshot files in messages" on page 42. Updateable snapshot messages are identified as SU types in the descriptions of checks that report them.

Warning: Mistakes in the Windows registry can cause serious system-wide problems. Update the Windows Emergency Repair diskette before making any changes.

Common Registry messages

When you run a policy that contains the Registry module, the module compares current registry information with the Registry templates before any checks are run. Registry templates are enabled in the Template file list option.

The following messages may be reported before checks are run.

Message name	Title	Class
ADDITIONAL_ SACL_ENTRY	Additional SACL entry	1
DIFFERENT_ SACL_ENTRY	Different SACL entry	1
FILE_MISSING	No template files specified	4
FORBIDDEN_ DATA	Registry value set to forbidden data	4
INFO	Registry information	0
MISSING_ SACL_ ENTRY	Missing SACL entry	1
NOEXISTVALUE	Mandatory registry value does not exist	4
VALUE_TYPE_CHANGED	Registry value type has changed	1
WRONG_DATA	Registry value set to incorrect data	4
WRONG_TYPE	Registry value set to incorrect type	4

Using wildcard characters

Standard wildcard usage is supported in the Registry template.

See "Editing an ACL sublist" on page 225, "Editing a Snapshot Values sublist" on page 226, "Editing a Check Values sublist" on page 227, "Editing a Value Info Queries sublist" on page 228, and "Editing a Skip Conditions sublist" on page 230.

Use the ? character to substitute for any one ASCII character in a string. Use the * character to substitute for any number of ASCII characters in a string.

Wildcards used as partial file or directory names such as fil*.bat and *.* are accepted.

In addition to the Registry template, standard wildcard usage is supported in:

- Name lists throughout Symantec ESM
  See "To add an item to a name list" on page 35.
- Startup Files
  See "Required services" on page 240, "Disallowed services" on page 241, and "Unknown services" on page 242.

In the Discovery module, wildcard characters are used differently to specify IP addresses.

See "Targets" on page 96.

Template file list

Use this option to enable or disable Registry template files that are used by Registry security checks.

The template types are:

- Windows Server 2003 .rs6
- Windows XP Professional .rwx
- Windows 2000 Professional .rw5
- Windows 2000 Server .rs5
- Windows NT 4.0 Server .rs4
- Windows NT 4.0 Workstation .rw4

Editing the Registry template

Registry templates are used to verify agent key and subkey attributes.

Three default templates are provided:

- Mime for mime buffer overflow vulnerability.
- Registry for registry vulnerability.
- VeriSign for fraudulent certificate vulnerability.

Do not edit Registry templates that are installed with Symantec ESM. Instead, add your own.

To add a new Registry template

1. In the enterprise tree, right-click **Templates**, then click **New**.
2. In the Create New Template dialog box, click one:
   - **Registry - Windows Professional**
   - **Registry - Windows Server**
3. Type a name for the module of no more than eight characters, without a file name extension. The extension is added automatically.
4. Load registry key information using any of three methods:
   - Load a single registry key. See "To load information for a single registry key" on page 222.
   - Load a registry key and its subordinates. See "To load information for a registry key and its subordinates" on page 223.
   - Manually enter registry key information. See "To manually enter registry key information" on page 223.
5. Click **Close** to exit the Template Editor.

To load information for a single registry key

1. If the Template Editor is not already open, double-click the name of the template in the enterprise tree.
2. In the Template Editor, click **Add Key**.
3. Click the Agent name field, then click the agent that has the key.
4. In the Item name field, type the path of the key on the agent computer.
5. Click **OK**.

To load information for a registry key and its subordinates

1. If the Template Editor is not already open, double-click the name of the module in the enterprise tree.
2. In the Template Editor, click **Add Key/Subkeys**.
3. Click the Agent name field, then click an agent that has the key.
4. In the Item to add field, type the path and name of the key on the agent.
5. Select the level of subordinate keys that you want to load. Each level includes all keys at that level.
   - **This level and all subordinates**
   - **This item only (no subordinates)**
   - **Include (number of subordinate levels)**

   For example, this setting loads all subkeys in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT key into the template:

   Do not load a non-existent key into the template.
6. Click **OK**.

To manually enter registry key information

1. If the Template Editor is not already open, double-click the name of the template in the enterprise tree.
2. Click **Add Key**.
3. In the Key Name field, replace <NEW> with the appropriate information.
4. In the Owner field, replace <NEW> with the appropriate information.
5. In the Comment field, replace <NEW> with the appropriate information.

   Text in the Comment field is displayed with the usual messages in the console grid when you run the module. However, text in any Comment field of any sublist on this row overrides this text.
6. Check or uncheck **Check Time** to turn this feature on or off
7. Check or uncheck **Enable ACL Checking** to turn this feature on or off.
8. Click the Required field, then click one of the following:
   - **Optional** Key must supersede at least one other key.
   - **Mandatory** Key must exist.
   - **Forbidden** Key must not exist.

9 In the Subkey Search field, replace <NEW> with one of the following values:

Value	Result
2	searches two levels of children
1	searches only one level of children
0	searches the key only, no children
-1	searches all children

Note: The Registry module searches all children on some critical registry keys. You can reduce policy run time by limiting subkey search depth.

10 Add entries to the following sublists as needed:

- ACL. See "To add a row to an ACL sublist" on page 225.
- Snapshot Values. See "To add a row to a Snapshot Values sublist" on page 226
- Check Values. See "To add a row to a Check Values sublist" on page 227.
- Value Info Queries. See "To add a row to the Value Info Queries sublist" on page 228.
- Data Existence. See "To add a row to a Data Existence sublist" on page 229.
- Skip Conditions See "To add a row to a Skip Conditions sublist" on page 230.
- Auditing See "To add a row to an Auditing sublist" on page 234.

11 Click **Save**.
To add another row, repeat steps 2–8.

12 Click **Close** to exit the Template Editor.

Editing an ACL sublist

ACL sublist entries contain registry key permissions that have been granted to security groups and users. For example, the Read permission may be granted to the %EVERYONE% group for HKEY_CURRENT_USER\Software. Wildcard characters * and ? are allowed.

To add a row to an ACL sublist

1. In the registry record that you are editing in the Template Editor, click the ACL sublist button (initially 0).
2. In the Template Sublist Editor, click **Add Row**.
3. In the User/Group field, replace <NEW> with the name of a user or security group.
4. In the Permissions field, replace <NEW> with values of permissions that have been granted to a user or security group on a file or folder. Valid entries are:

Permission	Value	Description
Read	Read QENC	Lets users read the values in a key
Full Control	Full Control QVSENLDPOC	Lets users read, modify, delete, or take ownership of a key
None		No permissions
Query	Q or q	Read a key value
Set Value	V or v	Set or modify a key value
Create Subkey	S or s	Add a subkey to a key
Enumerate Subkey	E or e	List the subkeys in a key
Notify	N or n	Open a key with notify access
Create Link	L or l	Add a link between keys
Delete	D or	Remove a key
Write DAC	P or p	Modify the ACL for a key
Write Owner	O or o	Take ownership of a key
Read Control	C or c	Read security data for a key

You can enter any combination of values in any order regardless of case (upper or lower). The Read value is an exception. It cannot be combined with any other value. Instead, use the QENC form. For example, the value of Read plus Create Link can be QENCL, LQencl, or lqencl, etc., but not ReadL.

5. In the Comment field, replace <NEW> with text that you want to display with messages in the console grid when you run the module.

   Comment text in any sublist overrides Comment text in the row that you are editing in the Registry template. All sublist comments are displayed when the Registry module is run.
6. Click **Apply**. To add another row, repeat steps 2–6.
7. Click **Close** to exit the Template Editor.

Editing a Snapshot Values sublist

Some keys and subkeys contain critical values, including REG_BINARY data such as encrypted passwords. These values are compared to the snapshot file data and any changes are reported. Wildcard characters * and ? are allowed.

If the Snapshot Values sublist has no entries, the module will not check for the presence of these values in the key.

To add a row to a Snapshot Values sublist

1. In the row that you are editing in the Template Editor, click the Snapshot Values button (initially **0**).
2. In the Template Sublist Editor, click **Add Row**.
3. In the Value Name field, replace <NEW> with a name to match the value in the key.
4. The Value Size and Value Type check boxes must be checked to report changes in value size and type.
5. To verify the CRC and/or MD5 signatures of specified registry values, click the Signature field (initially None), then click one of the following:
   - **CRC** 16-bit signature
   - **MD5** 128-bit signature
   - **CRC+MD5** Combined CRC and MD5
6. To require or prohibit the specified value, click the Required field (initially **Optional**), then click one:
   - **Mandatory** Key must exist.
   - **Forbidden** Key must not exist.

The Optional setting makes the comparison for the snapshot if the value is present. If it is not present, but added later, the addition is reported.

7 In the Comment field, replace <NEW> with text that you want to display with messages in the console grid when you run the module.
Comment text in any sublist overrides Comment text in the row that you are editing in the Registry template. All sublist comments are displayed when the Registry module is run.

8 Click **Apply**.
To add another row, repeat steps 2–8.

9 Click **Close** to exit the Template Editor.

Editing a Check Values sublist

Some keys and subkeys contain multiple values of different types. The Key and value existence check uses information that is stored in this sublist to identify key values of the wrong type and non-existent values. Wildcard characters * and ? are allowed.

If this sublist has no entries for a key, the module ignores key values.

To add a row to a Check Values sublist

1 In the row that you are editing in the Template Editor, click the Check Values button (initially 0).

2 In the Template Sublist Editor, click **Add Row**.

3 In the Value Name field, replace <NEW> with a name for the value in the key.

4 Click the Value Type field (initially String Value), then click a value:

Value type	Description
String Value	Unicode string
Binary Value	Free form binary
WORD Value	32-bit number
EXPAND_SZ	Unicode string with environment variable references
WORD_BIG_ENDIAN	32-bit number (Big_Endian)
LINK	Symbolic link (unicode)
MULTI_SZ	Multiple unicode strings
RESOURCE LIST	Resource list in the resource map

Value type	Description
FULL_RESOURCE_DESCRIPTOR	Resource list in the hardware description
NONE	No value type

5. In the Value Data Regular Expression field, do one of the following:
   - To ignore the data in key values, delete <NEW>.
   - To look for specific data in the key value, replace <NEW> with a regular expression. See "Using regular expressions" on page 231. You can also use comparison operators <, >, <=, >=, and !=.
6. In the Comment field, replace <NEW> with text that you want to display with messages in the console grid when you run the module.

   Comment text in any sublist overrides Comment text in the row that you are editing in the Registry template. All sublist comments are displayed when the Registry module is run.
7. Click **Apply**. To add another row, repeat steps 2–7.
8. Click **Close** to exit the Template Editor.

Editing a Value Info Queries sublist

Some keys and subkeys contain values that should be monitored. Wildcard characters * and ? are allowed. If the Value Info Queries sublist has no entries, the module does not check for the presence of these values in the key.

To add a row to the Value Info Queries sublist

1. In the row that you are editing in the Template Editor, click the Values Info Queries button (initially **0**).
2. In the Template Sublist Editor, click **Add Row**.
3. In the Key Name field, replace <NEW> with the name key name of the row that you are editing.
4. In the Value Name field, replace <NEW> with a name for the subkey value.
5. In the Comment field, replace <NEW> with text that you want to display with messages in the console grid when you run the module.

   Comment text in any sublist overrides Comment text in the row that you are editing in the Registry template. All sublist comments are displayed when the Registry module is run.
6. Click **Apply**. To add another row, repeat steps 2–6.
7. Click **Close** to exit the Template Editor.

Editing a Data Existence sublist

Some keys or subkeys, such as Enable Plain Text Password, reduce system security.

Forbidden keys must not have values. Required keys, on the other hand, must have values that match a specified regular expression.

If this sublist contains no entries, the Registry module ignores the existence of data in keys.

To add a row to a Data Existence sublist

1. In the row that you are editing in the Template Editor, click the Data Existence button (initially 0).
2. In the Template Sublist Editor, click **Add Row**.
3. In the Key Name and Value Name fields, replace <NEW> with the corresponding name and value in the subkey.
4. In the Value Data Regular Expression field:
   - To look for specific data in the key values, replace <NEW> with a regular expression. See “Using regular expressions” on page 231.

     You can also use comparison operators <, >, <=, >=, and !=, and wildcard characters * and ?
   - If you do not want to look for specific data, delete <NEW>.
5. If data is prohibited, click the Required field (initially Mandatory), then click **Forbidden**.
6. In the Comment field, replace <NEW> with text that you want to display with messages in the console grid when you run the module.

   Comment text in any sublist overrides Comment text in the row that you are editing in the Registry template. All sublist comments are displayed when the Registry module is run.
7. Click **Apply**. To add another row, repeat steps 2–7.
8. Click **Close** to exit the Template Editor.

Editing a Skip Conditions sublist

Some keys or subkeys do not apply to the computer. In situations where the value name matches the regular expression, there is nothing to check so the module skips the key. Wildcard characters * and ? are allowed.

If the Skip Conditions sublist has no entries, the module will not skip the conditions when checking the key.

To add a row to a Skip Conditions sublist

1. In the row that you are editing in the Template Editor, click the Skip Conditions button (initially **0**).
2. In the Template Sublist Editor, click **Add Row**.
3. Click the Condition button (initially **Key Exists**), then select the condition that you want to cause the module to skip the key:
   - **Key Exists**
   - **Key Does Not Exist**
   - **Value Exists**
   - **Value Does Not Exist**
   - **Data Matches**
   - **Data Does Not Match**
4. In the Key Name field, replace <NEW> with a subkey name to be matched.
5. In the Value Name field, replace <NEW> with a value name to be matched.
6. In the Value Data Regular Expression field:
   - To look for specific data in the key values, replace <NEW> with a regular expression. See “Using regular expressions” on page 231.
   - If you do not want to look for specific data, delete <NEW>.
7. In the Comment field, replace <NEW> with text that you want to display with messages in the console grid when you run the module.
   Comment text in any sublist overrides Comment text in the row that you are editing in the Registry template. All sublist comments are displayed when the Registry module is run.
8. Click **Apply**.
   To add another row, repeat steps 2–8.
9. Click **Close** to exit the Template Editor.

Using regular expressions

Use regular expressions to specify search patterns when checking data in registry key or subkey values. A regular expression is a sequence of characters, numbers, and/or operators.

Pattern	Description
. (period)	Matches any one character
\ (backslash)	Take the next character literally. Used if the character you want to match is a special character, for example: (ex: *, +, ?)
*	Matches zero or more occurrences of the previous atom. An atom is a regular expression in parentheses, a single character, a single character preceded by a backslash, or a range.
+	One or more occurrences of the previous atom
?	Zero or one occurrences of the previous atom
(...)	Used to enclose a part of the regular expression to be considered as an atom when applying *, +, ?, or the | (vertical bar) operator
[<char1><char2>...]	A range that matches any one of the characters that is listed in the range
[›...]	A range that matches any one character that is not listed in the range
[<char1>-<char2>...]	A range that matches any character in the range of ASCII characters from char1 to char2
| (vertical bar)	Or operator. The expression matches if either the atom before or after this character matches
<	Matches the beginning of a word in the string. Words are separated by white space.
>	Matches the end of a word in the string. Words are separated by white space.
›	Matches the beginning of the string
$	Matches the end of the string

If you do not include › or $, a match can occur anywhere in the string. For example, the regular expression abc matches the string mdabcijklm because the string contains a, b, and c in that order.

If you include > at the beginning and $ at the end of a regular expression, it can match only the specified string. For example, the regular expression >abc$ matches only abc. In most instances, start a regular expression with > and end with $.

Pattern	Results
.*	Anything
>.*	Anything
0+	Matches one or more zeros anywhere in a string. This regular expression matches: 0 1234567890 There are 000 ducks in the pond The expression does not match: abc 12387437 There are 456 ducks in the pond
>0*[1-9]+$	Matches zero or more zeros followed by one or more digits in the range 1-9. This regular expression matches: 0000001 21837717638 0012 The expression does not match: 1234567890 123.87437 00
(hatch)|(batch)	Matches any string containing hatch or batch. This regular expression matches: A batch of cookies schatching can you hatch a batch? The expression does not match: Down the Hatch One more latch
[Hh]atch	Any string containing Hatch or hatch

Pattern	Results
>[Aa][Nn][Yy]$	The word “any” in any combination of upper or lower case. This regular expression matches: ANY any aNy The expression does not match: Are there any more? (>/$ around a regular expression requires the expression to match the entire string)
[>0-9]	Any string containing at least one character that is not a digit
>[>0-9]$	Any single character that is not a digit
>[>0-9]*$	Any string that does not contain any digits
>(aba)+cde$	Matches any string containing one or more occurrences of “aba” followed by “cde”. This regular expression matches: abacde abaabacde abaabaabaabaabaabaabacde The expression does not match: abaxyzcde abacdecde
>aba+cde$	Matches any string containing one or more occurrences of “ab” followed by one or more “a” characters, followed by “cde”. This regular expression matches: abacde abaaaaaaacde The expression does not match: abaabaabaabaabaabaabacde abcde

Editing an Auditing sublist

Auditing registry keys and subkeys can help identify the source of unauthorized activities. The Auditing sublist stores success and failure settings for audits of critical access events.

If an Auditing sublist contains no entries, any encountered SACLs are reported as additional SACLs.

To add a row to an Auditing sublist

1. In the row that you are editing in the Template Editor, click the Auditing field (initially 0).
2. In the Template Sublist Editor, click **Add Row**.
3. In the User/Group field, replace <NEW> with the name of the user or security group.
4. In the Success field, replace <NEW> with events that you want the computer to audit if the user is successful. Valid entries are:
   - **All**
   - **None**
   - One or more of the following values in any order:

Value	Description
Q	Query value - read a key value
V	Set value - set or modify a key value
S	Create subkey - add a subkey to a key
E	Enumerate subkey - list the subkeys of a key
N	Notify - open a key with notify access
L	Create link - add a link between keys
D	Delete - remove a key
P	Write DAC - modify the ACL for a key
C	Read control - read security data for a key

Entries are not case sensitive.

5. In the Failure field, replace <NEW> with events that you want the computer to audit if the user is not successful. Valid entries are:
   - **All**
   - **None**
   - A combination of custom key entries as in step 4.
6. Click **Apply**.
   To add another row, repeat steps 2–8.
7. Click **Close** to exit the Template Editor.

Key ownership

This security check reports registry key ownership that changed after the last snapshot update.

Registry key owners can access, modify, and delete configuration information. Unauthorized changes can compromise system integrity and prevent legitimate users from accessing needed programs or resources.

The check returns the following messages:

Message name	Title	Type	Class
NOOWNER	Account specified in template does not exist on system		1
VALUE_TYPE_CHANGED	Registry value type has changed	SU	1
NOMATCH_PRIV_ENTRY	Privileged user ACL entry does not match		1
WRONG_KEY_OWNER	Different key ownership		4

To protect your computers

◆ Do one of the following:
   - For authorized changes, update the snapshot in the console grid.
   - For unauthorized changes, restore the correct settings manually.

Key permissions

This security check reports changes in registry key permissions.

In the Registry template, Ensure that **Enable ACL Checking** is checked.

The check returns the following messages.

Message name	Title	Type	Class
ADDITIONAL_ENTRY	Additional ACL entry	C in NT	1
CANNOT_GET_AUDITING_ INFO	Auditing ACL not checked		3
DIFFERENT_ENTRY	Different ACL entry	C in NT	1
MISSING_ENTRY	Missing ACL entry	C in NT	1
NOMATCH_PRIV_ ENTRY	Pivoted user ACL entry does not match		1
VALUE_TYPE_CHANGED	Registry value type has changed	SU	1

To protect your computers

◆ Do one of the following:

- Windows NT: For unauthorized additions, changes, or deletions, use the Correct function in the console grid to restore the previous ACLs.
- Windows 2000/XP: For unauthorized additions, changes, or deletions, manually restore the previous ACLs.

Key and value existence

This security check reports mandatory keys and values that do not exist, and forbidden keys and values that do exist.

The presence of forbidden keys or values can provide intruders with access to critical data such as user passwords. Missing mandatory registry keys can deny authorized users access to programs and other needed resources.

The check also uses Check Values sublist entries in the Registry template to identify key values of the wrong type or key values that do not exist.

The check returns the following messages:

Message name	Title	Type	Class
FORBIDKEY	Forbidden registry key exists		4
FORBIDVALUE	Forbidden registry value exists		4
NOEXISTKEY	Mandatory registry key does not exist		4
NOEXISTVALUE	Mandatory registry value does not exist		4
VALUE_TYPE_CHANGED	Registry value type has changed	SU	1
WRONG_DATA	Registry value set to incorrect data		4
WRONG_TYPE	Registry value set to incorrect type		4

To protect your computers

◆ Do one of the following:

- If a forbidden key is reported, delete it.
  If the key should not be forbidden, manually update the template.
- If a forbidden value is reported, delete it.
  If the value should not be forbidden, manually update the template.
- If a mandatory key does not exist, create it on the agent.
  If the key should not be required, manually update the template.
- If a mandatory value does not exist, create it on the agent. Set the value data to match the regular expression format that is reported in the Information field.
- If a value type changed and the change is authorized, update the snapshot.
  If the change is unauthorized, restore the previous type.
- If the registry data is incorrect, change it to match the regular expression that is specified in the template.
  If the data is correct, manually update the template.
- If the value type is incorrect, change the type to match the type specified in the template.
  If the type is correct, manually update the template.

Changed key (time)

This security check reports registry keys that changed, according to the last write time, after the last snapshot update.

The Check Time check box must be checked in the Registry template.

A change in the last write time indicates the registry key setting has changed.

The check returns the following message:

Message name	Title	Type	Class
KEY_LAST_WRITE	Registry key last write time has changed	SU	1
VALUE_TYPE_CHANGED	Registry value type has changed	SU	1

To protect your computers

- Do one of the following:
  - For authorized changes, update the snapshot in the console grid.
  - For unauthorized changes, restore the previous setting.

Changed value (size)

This check reports registry values that changed, according to the value data size, after the last snapshot update.

The Value Size check box must checked be in the Snapshot Values sublist of the Registry template.

The check returns the following message:

Message name	Title	Type	Class
VALUE_SIZE_CHANGED	Registry value size has changed	SU	1
VALUE_TYPE_CHANGED	Registry value type has changed	SU	1

To protect your computers

- Do one of the following:
  - For authorized changes, update the snapshot in the console grid.
  - For unauthorized changes, restore the correct settings manually.

Changed value (signature)

This check reports registry values that changed, according to value data signatures (CRC and/or MD5), after the last snapshot update.

The Signature option in the associated template record must not be None.

The check returns the following message:

Message name	Title	Type	Class
VALUE_SIGNATURE_CHANGED	Registry value signature has changed	SU	1
VALUE_TYPE_CHANGED	Registry value type has changed	SU	1

Note: This check is difficult for hackers to circumvent, but the Registry module runs faster when this check is disabled.

Response

The Response module detects vulnerabilities using templates in Symantec ESM response policies. Response policies are configured by the Symantec Security Response team to respond quickly to new security incidents and vulnerabilities between regular security update releases. Response module templates cannot be created or edited by users.

Startup Files

The Startup Files module reports information about system services, run keys, and remote registry access.

Warning: Improperly modifying the Windows registry can cause serious, system-wide problems. Update the Windows Emergency Repair diskette before making any changes.

Some messages report messages that you can use to update template or snapshot files to match current agent settings. See “Updating template and snapshot files in messages” on page 42. Other checks report messages that you can use to reverse agent settings or disable user accounts. See “Correcting agents in messages” on page 42. Updateable and correctable messages are identified as TU, SU, or C type messages in the descriptions of checks that use them.

Installed services

This security check reports all services that are installed on the agent.

The check returns the following message:

Message name	Title	Class
LIST	List installed services	0

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Installed services.
2. Run the demo policy on the agent.
3. Verify that List installed services is reported.

To protect your computers

- Remove any unauthorized or unnecessary services.

Required services

This security check reports stopped or missing services that you have specified as required in the name list.

In the name list, type the service or display name of startup services that should be running. Wildcard characters (? and *) are accepted.

Note: If you are running Disallowed services or Unknown services at the same time, and the name list for either of them contains a required service, a red level message is reported.

The check returns the following messages:

Message name	Title	Type	Class
REQNOTFND	Required services not installed		4
REQNOTRUN	Required services not running	C	4
DUPSVCNAME	Service named by more than one check		4

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Required services.
2. Edit the name list in the Required services check:
   - Add the name of a service that is not currently installed.
   - Add the name of an installed but stopped service.
3. Run the demo policy on the agent.
4. Verify that Required services not installed is reported for both services that you added to the name list.

To protect your computers

- ◆ Do one of the following:
  - For a required service that is not running, use the Correct feature in the console grid to restart it.
  - Set the startup type of required services to Automatic.
  - When a service is reported in more than one enabled check name list, remove the service from all but one, then run the module again.

Disallowed services

This security check reports running or installed services that you have specified as disallowed. These services should not be installed or started without the approval of the system administrator.

In the name list, type the service or display names of disallowed services. Wildcards characters (* and ?) are accepted.

Note: If you are running Required services or Unknown services at the same time, and the name list for either of them contains a disallowed service, a red level message is reported.

The check returns the following messages:

Message name	Title	Type	Class
DISALLOWNOTRUN	Disallowed services installed		1
DISALLOWRUN	Disallowed services running	C	4
DUPSVCNAME	Service named by more than one check		4

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Disallowed services.
2. Edit the name list in the Required services check:
   - Add the name of an installed but stopped service.
   - Add the name of an installed and running service.
3. Run the demo policy on the agent.
4. Verify that Disallowed services installed and Disallowed services running are reported for the appropriate services.

To protect your computers

◆ Do one of the following:

- For a disallowed service, use the Correct feature in the console grid to stop it, then set its Startup method to Disabled.
- When a service is reported in more than one enabled check name list, remove the service from all but one, then run the module again.

Unknown services

This security check reports installed services that are not listed as Optional services in the name list for this check nor as Required or Disallowed services in the name lists for other module checks.

Enable both the Required and Disallowed Services checks when you run this check to ensure that required or disallowed services are not reported as unknown services.

In the name list, type the service or display name of a startup service. Wildcard characters (* and ?) are accepted.

Note: If you are running Required services or Disallowed services at the same time, and the name list for either of them contains an optional service, a red level message is reported.

The check returns the following messages:

Message name	Title	Type	Class
UNKNOWNRUN	Unknown service running	C	4
UNKNOWNNOTRUN	Unknown service installed		1
DUPSVCNAME	Service named by more than one check		4

To protect your computers

- Do one of the following:
  - For unknown running services, use the Correct feature in the console grid to stop the service, then set its Startup type to Disabled.
  - Remove unknown services that are not authorized.
  - Consider adding authorized services to the Include name list for the Required services check or the Exclude name list for this check. Also add any unauthorized services to the Include list for the Disallowed services check.
  - When a service is reported in more than one enabled check name list, remove the service from all but one name list, then rerun the module.

Changed services

This security check reports service configuration changes that were made after the last snapshot update.

The check returns the following updateable message:

Message name	Title	Type	Class
CHGSERVICE	Changed service	SU	1

To demonstrate the check

1. If you have not already done so, run the Startup Files module in the demo policy to create the baseline snapshot.
2. In the demo policy, disable all checks in the Startup files module except Changed services.
3. Change the starting type of a service on the agent. For example, change the starting type of the Alerter service from manual to disabled.
4. Run the demo policy on the agent.
5. Verify that Changed service is reported for the Alerter service.

To protect your computers

- Do one of the following:
  - For authorized changes, update the snapshot in the console grid.
  - For unauthorized changes, restore the correct service configuration.

New services

This security check reports any new services that were added after the last service snapshot update.

The check returns the following updateable message:

Message name	Title	Type	Class
NEWSERVICE	New service installed	SU	1

To demonstrate the check

1. If you have not already done so, run the Startup Files module in the demo policy to create the baseline snapshot.
2. In the demo policy, disable all checks in the Startup Files module except New services.
3. Add a new service on the agent.
4. Run the demo policy on the agent.
5. Verify that New service installed is reported.

To protect your computers

- Do one of the following:
  - For authorized service additions, update the snapshot in the console grid.
  - Remove unauthorized services.

Deleted services

This security check reports services that were deleted after the last services snapshot update.

The check returns the following updateable message:

Message name	Title	Type	Class
DELSERVICE	Deleted service	SU	0

To demonstrate the check

1. If you have not already done so, run the Startup Files module in the demo policy to create the baseline snapshot.
2. In the demo policy, disable all checks in the Startup Files module except Deleted services.
3. Delete a service on the agent.
4. Run the demo policy on the agent.
5. Verify that Deleted service is reported.

To protect your computers

- ◆ Do one of the following:
  - For authorized deletions, update the snapshot in the console grid.
  - Reinstall any unauthorized service deletions.

Services using system account to run

This security check reports services that run under the system account.

Many services run under the local system account. This account has full access to the system. Intruders can attack nonessential services and gain access to the local system account.

The check returns the following message:

Message name	Title	Class
SVCSYSACC	Service using System account to run	1

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Services using system account to run.
2. Run the demo policy on the agent.
3. Verify that Service using System account to run is reported.

To protect your computers

- ◆ Change all services that are not required by the Local System account to accounts with limited privileges.

Services using specified user accounts to run

This security check reports services that use specified accounts to run.

The name lists let you exclude or include users and security groups for the check.

The check returns the following message:

Message name	Title	Class
SVCUSERACC	Service using specified user account to run	0

To demonstrate the check

1. In a demo policy, disable all Startup Files module checks except Services using specified user accounts to run.
2. Change the System Event Notification service to log on using a local test user account.
3. In the Services using specified user accounts to run check:
   - Click **Include these Users/Groups**.
   - Delete all user accounts in the name lists.
   - Add the local test user account name to the included Users name list.
4. Run the demo policy on the agent.
5. Verify that Service using specified user account to run is reported.

To protect your computers

- Use system accounts to run services.

Contents of Run keys

This security check reports the contents of registry Run keys. Programs in Run keys execute automatically on startup.

Trojan horse attacks often use Run keys to run executables at startup.

Use the name list to specify files that you do not want to be reported.

The check returns the following message:

Message name	Title	Type	Class
RUN_KEY_ENTRY	Run key entry	C	0

To demonstrate the check

1. In a demo policy, disable all Startup Files module checks except Contents of Run keys.
2. In the check name list, delete Run key entries.
3. Run the demo policy on the agent.
4. Verify Run key entry is reported for each executable that runs automatically at startup.

To protect your computers

- In the console grid, use the Correct feature to remove unauthorized executables from the registry Run key.

Remote Procedure Call (RPC) disabled

This security check reports if the Remote Procedure Call (RPC) subsystem is enabled. This enables execution of remote requests.

The check returns the following message:

Message	Title	Class
RPCENABLE	Remote Procedure Call (RPC) enabled	1

To demonstrate the check

1. In a demo policy, disable all Startup Files module checks except Remote Procedure Call (RPC) disabled.
2. Verify that the Remote Procedure Call (RPC) and Remote Procedure Call (RPC) Locator services are started.
3. Run the demo policy.
4. Verify that Remote Procedure Call (RPC) enabled is reported for the RPC locator and service.

To protect your computers

- Ensure that the RPC gives only authorized permissions to accounts.

Remote registry access

This security check reports accounts that can access the registry remotely. 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.

When a user establishes a remote connection to the registry, the security on the individual keys is the only thing that restricts user access, regardless of what permissions the user is granted on the winreg key.

Use the name list to include or exclude accounts for this check.

The check returns the following message:

Message	Title	Class
RMTREGISTRY_PERMISSIONS	Users/Groups found with remote registry permissions	4

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Remote registry access.
2. Run regedt32.exe and access the HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg key in the registry.
3. On the Menu bar, click **Security** > **Permissions**.
4. Ensure that the Everyone group has Read access.
5. Run the demo policy on the agent.
6. Verify that Users/Groups found with remote registry permissions is reported.

To protect your computers

- Disable remote access to the registry for all users except administrators.

Remote registry access (anonymous) (Windows NT)

This check reports a problem if anonymous connections can remotely access the registry. If the Everyone group has Read or Write access to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg key, the registry can be accessed through anonymous connections.

After a user has established a remote connection to the registry, only the security on individual keys restricts the user's access, regardless of what permissions the user is granted on the winreg key.

The check returns the following message:

Message	Title	Type	Class
RMTREGISTRY_ ANONYMOUS	Remote registry permissions allow anonymous access to registry	C	4

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Remote registry access (anonymous).
2. Run regedt32.exe and access the HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\ SecurePipeServers\winreg key in the registry.
3. On the Menu bar, click **Security** > **Permissions**.
4. Ensure that ANONYMOUS LOGON has Read access.
5. Run the demo policy on the agent.
6. Verify that Remote registry permissions allow anonymous access to registry is reported.

To protect your computers

◆ In the console grid, use the Correct feature to remove the access control entry for the ANONYMOUS LOGON security group from the winreg key.

Remote registry access (non-Administrators) (Windows NT)

This check reports a problem if any account that is not a member of the Administrators security group can remotely access the registry.

Any user granted Read or Write access to the KEY_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, only the security on individual keys restricts the user's access, regardless of what permissions the user is granted on the Winreg key.

Disabling remote registry access can prevent legitimate remote administration of the system or prevent remote software upgrades.

Because this is the most restrictive remote registry check, you may want to disable it.

The check returns the following message:

Message	Title	Type	Class
RMTREGISTRY	Remote registry access enabled	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the Startup Files module except Remote registry access (non-Admnistrators).
2. Run regedt32.exe and access the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg key in the registry.
3. On the Menu bar, click **Security** > **Permissions**.
4. Ensure that the Everyone group has Read access.
5. Run the demo policy on the agent.
6. Verify that Remote registry access enabled is reported.

To protect your computers

- Do one of the following:
    - In the console grid, use the Correct feature to delete user remote ACL entries.
    - Remove Everyone from the winreg registry setting.

Symantec Product Info

The Symantec Product Info module reports a problem if Symantec AntiVirus Corporate Edition or Norton AntiVirus is not installed on the agent. It also reports a problem if their version number, last scan time, or last LiveUpdate time are not within the limits that you specify. Symantec AntiVirus Enterprise Edition is a standalone product and is also included in Symantec AntiVirus Enterprise Edition.

Note: In the Symantec ESM console, the checks for this module are organized under Symantec AntiVirus Corporate Edition and Norton AntiVirus headers. Checks are named Minimum version, LiveUpdate frequency and Scan frequency under each header. In this document, checks present product names in parentheses for easy reference.

Minimum version (Norton AntiVirus)

This security check reports a problem if the version number of the agent's Norton AntiVirus is less than the version that you specify in the check, or if the application is not installed.

The check accepts one-, two-, or three-part version numbers (major, minor, and build numbers delimited by dot (period) characters).

Alpha characters and non-dot punctuation end the number. For example, if the installed version is 8.01 and you specify eight, the number is treated as zero and Norton AntiVirus version outdated is reported.

Omitted part numbers are treated as zeros. For example, if the installed version is 8.01 (a two-part number) and you specify 8, nothing is reported.

Extra numbers are truncated. For example, if the installed version is 8.01 (a two-part number) and you specify 8.01.5, nothing is reported.

The check returns the following message:

Message	Title	Class
AV_VERSION_VIOLATION	Norton AntiVirus version outdated	4
AV_NOT_INSTALLED	Norton AntiVirus not installed	4

To protect your computers

- Keep anti-virus software current.

LiveUpdate frequency (Norton AntiVirus)

This security check reports a problem if LiveUpdate has not been run for Norton AntiVirus software within the number of days that you specify in the check.

The check returns the following message:

Message	Title	Class
AV_LU_VIOLATION	Norton AV LiveUpdate overdue	3
AV_NOT_INSTALLED	Norton AntiVirus not installed	4

To protect your computers

- Run LiveUpdate for Norton AntiVirus every 7 days.

Scan frequency (Norton AntiVirus)

This security check reports a problem if the number of days since the last Norton AntiVirus scan is greater than the number of days that you specify in the check.

The check returns the following message:

Message	Title	Class
AV_LASTSCAN_VIOLATION	Norton AntiVirus scan overdue	3
AV_NOT_INSTALLED	Norton AntiVirus not installed	4

To protect your computers

- Scan for viruses at least every 7 days.

Minimum version (Symantec AntiVirus Corporate Edition)

This security check reports a problem if the agent's Symantec AntiVirus Corporate Edition version number is less than the version number that you specify in the check, or if the application is not installed.

The check returns the following messages:

Message	Title	Class
AVCE_VERSION_VIOLATION	Symantec AntiVirus Corporate Edition version outdated	4
AVCE_NOT_INSTALLED	Symantec AntiVirus Corporate Edition not installed	4

To protect your computers

- Keep anti-virus software current.

LiveUpdate frequency (Symantec AntiVirus Corporate Edition)

This security check reports a problem if the agent has not run LiveUpdate for Symantec AntiVirus Corporate Edition software within the number of days that you specify in the check.

The check returns the following messages:

Message	Title	Class
AVCE_LU_VIOLATION	Symantec AntiVirus Corporate Edition LiveUpdate overdue	3
AVCE_NOT_INSTALLED	Symantec AntiVirus Corporate Edition not installed	4

To protect your computers

- Run LiveUpdate for Symantec AntiVirus Corporate Edition every 7 days.

Scan frequency (Symantec AntiVirus Corporate Edition)

This security check reports a problem if the number of days since the last Symantec AntiVirus Corporate Edition scan is greater than the number of days that you specify in the check.

The check returns the following messages:

Message	Title	Class
AVCE_LASTSCAN_VIOLATION	Symantec AntiVirus Corporate Edition scan overdue	3
AVCE_NOT_INSTALLED	Symantec AntiVirus Corporate Edition not installed	4

To protect your computers

- Scan for viruses at least every 7 days.

System Auditing

The System Auditing module reports security events that are audited for failure or success and what happens when the log file is full.

System auditing helps you identify unauthorized users and provides valuable tracking information during or after a break-in.

Some checks report messages that you can use to update template or snapshot files to match current agent settings. See “Updating template and snapshot files in messages” on page 42. Other checks report messages that you can use to reverse agent settings or disable user accounts. See “Correcting agents in messages” on page 42. Updateable and correctable messages are identified as TU, SU, or C type messages in the descriptions of checks that use them.

Security events success auditing

This security check reports events that, according to the Enabled Keys list, should be audited for successful attempts but are not being audited. Without this information, system administrators cannot track unauthorized activities during or after a break-in.

Use the Keys list to specify which successful security events should be audited.

The check returns the following messages:

Message name	Title	Type	Class
SEC_EVENT_AUDIT_NOT_ENABLED	Security event auditing is not enabled	C	4
SEC_EVENT_SETTING_TOO_WEAK	Security event audit settings are too weak	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the System Auditing module except Security events success auditing.
2. Set the Windows Audit Policy not to audit logon activity (for Windows NT, Logon and Logoff).
3. In the check's name lists do one of the following:
   - Windows NT: Enable the Logon and Logoff key.
   - Windows 2000/XP: Enable logon events.
4. Run the demo policy on the agent.
5. Verify that Security event audit settings are too weak is reported.
6. Set the Windows Audit Policy not to audit any activity.
7. Run the demo policy on the agent.
8. Verify that Security event auditing is not enabled is reported.

To protect your computers

- ◆ Use the Correct feature in the Updateable/Correctable field of the console grid to enable auditing for reported events.

Security events failure auditing

This check verifies that specified, failed security events are audited.

Use the Keys lists to specify which failed security events should be audited.

Without auditing information, you cannot track activity during or after a break-in.

The check returns the following messages:

Message name	Title	Type	Class
SEC_EVENT_AUDIT_NOT_ENABLED	Security event auditing is not enabled	C	4
SEC_EVENT_SETTING_TOO_WEAK	Security event audit settings are too weak	C	1

To demonstrate the check

1. In a demo policy, disable all System Auditing module checks except Security events failure auditing.
2. Set the Windows Audit Policy not to audit logon failure activity (for Windows NT, Logon and Logoff).
3. In the check's name lists do one of the following:
   - Windows NT: Enable the Logon and Logoff key.
   - Windows 2000/XP: Enable logon events.
4. Run the demo policy on the agent.
5. Verify that Security event audit settings are too weak is reported.
6. Set the Windows Audit Policy not to audit any activity.
7. Run the demo policy on the agent.
8. Verify that Security event auditing is not enabled is reported.

To protect your computers

- Use the Correct feature in the Updateable/Correctable field of the console grid to enable event auditing.

Security events do not overwrite security log

This security check reports a problem if the system can overwrite the security event log.

Without the information that is stored in the security event log, you cannot track unauthorized activities during or after a break-in.

The check returns the following message:

Message name	Title	Type	Class
LOG_OVERWRITE	Security event log will be overwritten	C	1

When the following conditions exist, your system starts storing audit events in memory, greatly slowing down activity on the system:

- Log file reaches its maximum size.
- System is not set to halt when the log file reaches its maximum size.
- Overwriting of the security log is prevented.

To demonstrate the check

1. In a demo policy, disable all System Auditing module checks except Security events do not overwrite security log.
2. Change the Windows <OS> Event Viewer Security Log settings to overwrite events when the log is full.
3. Run the demo policy on the agent.
4. Verify that Security event log will be overwritten is reported.

To protect your computers

◆ Use the Correct function in the console grid to change the value of the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\Retention key so that the log can only overwrite events that are older than the archive period in your security policy (FFFFFFFF hex).

System halts when security log full

This security check reports a problem when a full security event log does not halt the system. The system continues to run without logging new security events.

Without the information that is stored in the security event log, you cannot track unauthorized activities during or after a break-in.

The check returns the following message:

Message name	Title	Type	Class
LOG_FULL_SYSTEM_NO_HALT	System does not halt when security event log full	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the System Auditing module except System halts when security log full.
2. Run Regedt32.exe and access the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa key in the Windows registry.
3. Ensure that the crashonauditfail key is not present or change its REG_DWORD value from 1 to 0.
4. Run the demo policy on the agent.
5. Verify that System does not halt when security event log full is reported.

To protect your computers

◆ Use the Correct feature of the console grid to change the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\crashonauditfail registry value to 1 so that the system halts when the log file is full.

Security event log size

This security check reports a problem when the security event log size is less than the size specified in the check. The default value is 512 kilobytes.

If the size of the log is too small, logged events can either be lost or the system can halt unexpectedly.

The check returns the following message:

Message name	Title	Type	Class
LOG_SIZE_SMALL	Security event log size is too small	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the System Auditing module except Security event log size.
2. In the Properties dialog box of Windows' Event Viewer Security Log, change the Maximum log size setting to 64 KB.

3. In the Security event log size check, specify a Log size of 512 kilobytes.
4. Run the demo policy on the agent.
5. Verify that Security event log size is too small is reported.

To protect your computers

◆ In the console grid, use the Correct feature to change the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\MaxSize registry value to at least 512 kilobytes.

Days until security events are overwritten

This security check reports a problem when the system starts to overwrite security event log entries in fewer than the specified number of days. The default value is 30 days.

Without the information that is stored in the security event log, you cannot track unauthorized activities during or after a break-in.

The check returns the following message:

Message name	Title	Type	Class
LOG_TIME_TO_OVERWRITE_TOO_SHORT	Security event log will be overwritten too soon	C	1

To demonstrate the check

1. In a demo policy, disable all checks in the System Auditing module except Days until security events are overwritten.
2. In the Properties dialog box of the Windows Event Viewer Security Log, change the Overwrite events older than setting to 1 day.
3. In the Days until security events are overwritten check, change Days to 30.
4. Run the demo policy on the agent.
5. Verify that Security event log will be overwritten too soon is reported.

To protect your computers

◆ In the console grid, use the Correct feature to change the value of registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\Retention to at least 30 days. The number of days is automatically converted to seconds.

User Files (Windows NT)

The User Files module examines user logon scripts, profiles, and home directories for proper access control.

Users to check (Windows NT)

Use this option to specify users and security groups that are excluded or included for all security checks in the module. See “Editing name lists” on page 35.

Disable Run on File menu (Windows NT)

This security check reports computers where the Run option on the Start menu is not disabled.

Users should have access only to the applications provided by the system administrator. If users can access the Run option in the Start Menu, they can execute any installed program.

You can use the name lists in the check to exclude users or groups that are not already excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
CHECK_NOT_PERFORMED	This check requires the Server service to be running	1
NOUNC	Universal Name Convention Is Used in File Names	1
PROFILE_NOT_EXIST	User profile does not exist	1
RUN_NOT_DISABLED	Run is not disabled in File menu	1

To protect your computers

- Do one of the following:
  - If the check cannot be performed, start the Server service.
  - If Universal Name Convention is used in file names, rename the files without using the \\computer format.
  - If the user profile does not exist, create or copy the user profile into the appropriate folder.
  - If Run is not disabled, disable it in the User Profile Editor.

Disable Saved/Never Save (Windows NT)

This security check reports computers where the Saved Settings and Never Save Settings options are not disabled.

When not disabled, users can use these options to change their profiles, which can disrupt normal activities for other share users.

You can use the name lists in the check to exclude users or groups that are not already excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
CHECK_NOT_PERFORMED	This check requires the Server service to be running	1
NOUNC	Universal Name Convention is used in file names	1
PROFILE_NOT_EXIST	User profile does not exist	1
RUN_NOT_DISABLED	Run is not disabled in File menu	1
SAVE_NOT_DISABLED	Saved Settings/Never Save Settings not disabled	

To protect your computers and provide necessary user access

- Do one of the following:
  - If the check cannot be performed, start the Server service.
  - If Universal Name Convention is used in file names, rename the files without using the \\computer format.
  - If the user profile does not exist, create or copy the user profile into the appropriate folder.
  - If Run is not disabled, disable it in the User Profile Editor.
  - If the Saved Settings and Never Save Settings are not disabled, disable them in the User Profile Editor.

Common program groups (Windows NT)

This security check reports computers that can access common program groups.

Use the name lists in the check to exclude users or groups.

The check returns the following messages:

Message name	Title	Class
CHECK_NOT_PERFORMED	This check requires the Server service to be running	1
NOUNC	Universal Name Convention is used in file names	1
COMMONGROUP_NOT_SHOWN	Common groups are not shown	1
PROFILE_NOT_EXIST	User profile does not exist	1
RUN_NOT_DISABLED	Run is not disabled in file menu	1

To protect your computers and provide necessary user access

- Do one of the following:
  - If the check cannot be performed, start the Server service.
  - If Universal Name Convention is used in file names, rename the files without using the \\computer format.
  - If common groups are not shown, enable Show Common Groups for appropriate user profiles in the User Profile Editor.
  - If the user profile does not exist, create or copy the user profile into the appropriate folder.
  - If Run is not disabled, disable it in the User Profile Editor.

Script ownership/access (Windows NT)

This check reports ownership of and access to imported or local logon script files. The files to be examined are defined by the file extensions that you specify in the Script file extensions to check option.

You can use the name lists in the check to exclude users or groups that are not already excluded by the Users to check option.

The check returns the following messages:

Message name	Title	Class
INVALID_SCRIPT_EXTENSION	Invalid file extension in logon script	1
NO_ACCESS_SCRIPT	No authorized access to logon script	1
NO_LOGON_SCRIPT	No logon script defined	1
NOUNC	Universal Name Convention is used in file names	1
OTHER_ACCESS_SCRIPT	Other users have unauthorized access to logon script	1

To demonstrate the check

1. In a demo policy, disable all checks in the User Files module except Script ownership/access.
2. If you have not already done so, add a test user to an agent computer.
3. Follow the procedure associated with the message that you want to demonstrate:

Message title	Procedure
Invalid file extension in logon script	Give a test logon script a .TST file extension.
No authorized access to logon script	Assign an invalid logon script to the test user.
Other users have unauthorized access to logon script	Give the test user Full Control permission to the logon script file.

4. Run the demo policy on the agent.
5. Verify that the appropriate message is reported.

To protect your computers and provide necessary user access

◆ Do one of the following:
  - If the logon script has an invalid file extension, rename it with the correct extension.
  - If no logon script has been defined, create one.
  - If Universal Name Convention is used in file names, rename the files without using the \\computer format.
  - If others have unauthorized access to a home directory, remove the permissions.

Script file extensions

This option specifies authorized file extensions for a logon script. Use the name list to specify additional extensions. The Script ownership/access check reports script files that do not have matching extensions.

Home folder ownership/access (Windows NT)

This security check reports a problem when a home folder does not exist, a user does not have a home folder, or a user does not have Full Control of the user's home folder.

You can use the name lists in the check to exclude users or groups that are not already excluded by the Users to check option.

To demonstrate the checkEnsure

1. In a demo policy, disable all checks in the User Files module except Home folder ownership/access.
2. If you have not already done so, add a test user to an agent computer.
3. Follow the procedure associated with the message that you want to demonstrate:

Message title	Procedure
Home folder missing	Delete the test user's home folder.
The user does not have ownership of the user's home folder	Revoke the test user's access to the home folder.
No authorized access to home folder	Revoke all access to the home folder.
System is not running NTFS/HPFS to support ACL	Create a home folder on a disk with a FAT partition.
Universal Name Convention Is Used in File Names	Create file names that use the \\ Universal Name Convention.
Other users have unauthorized access to home folder	Give an unauthorized user full access the the test user's home folder.

4. Run the demo policy on the agent.
5. Verify that the appropriate message is reported.

The check returns the following messages:

Message name	Title	Class
HOME_DIR_NOT_EXIST	Home folder missing	1
HOME_DIR_NOT_OWNED_BY_USER	The user does not have ownership of the user's home folder	1
NO_ACCESS_HOME_DIR	No authorized access to home folder	1
NO_ACL_SUPPORT	System is not running NTFS/HPFS to support ACL	1
NOUNC	Universal Name Convention is used in file names	1
OTHER_ACCESS_HOME_DIR	Other users have unauthorized access to home folder	

To protect your computers and provide necessary user access

- Do one of the following:
  - If the user does not have a home folder, create one in Windows Explorer and assign it to the user.
  - If the user does not own the user's home folder, assign it to the user.
  - If the home folder exists but the user does not have ownership, assign it to the user.
  - If the computer is not running NTFS/HPFS, convert the drive to NTFS for security purposes.
  - If Universal Name Convention is used in file names, rename the files without using the \\computer format.
  - If others have unauthorized access to a home directory, remove the permissions.

Suspicious files in folder (Windows NT)

This check reports a problem when copies of EXE, BAT, and/or CMD files that are in system folders are also in the user's home folder. Accessing this folder may interfere with normal operations.

You can use the name lists in the check to exclude users or groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
SUSPICIOUS_FILE	Suspicious files in user's home folder	1

To demonstrate the check

1. In a demo policy, disable all checks in the User Files module except Suspicious files in folder.
2. If you have not already done so, add a test user to an agent computer.
3. Copy a EXE, BAT, or CMD file and paste it into the home folder.
4. Rename the copied file to match the name of the original file.
5. Run the demo policy on the agent.
6. Verify that Suspicious files in user's home folder is reported.

To protect your computers

- Determine the reason for the file's presence in the home folder, then do one of the following:
  - If the file is not needed in the home folder, move, rename, or delete it.
  - If the file is needed in the home folder, add the user's name to the check's name list.

Logon script required (Windows NT)

This check reports users that do not have a logon script and therefore cannot access the network.

You can use the name lists in the check to exclude users or groups that are not already excluded by the Users to check option.

The check returns the following message:

Message name	Title	Class
NO_LOGON_SCRIPT	No logon script defined	1

To demonstrate the check

1. In a demo policy, disable all checks in the User Files module except Logon script required.
2. If you have not already done so, add a test user without a logon script.
3. Run the demo policy on the agent.
4. Verify that No logon script defined is reported.

To protect your computers

- Do one of the following:
  - If no logon script has been defined for a user, assign the user to a logon script.
  - If the user is not needed, delete the user.

Appendix

Integrated Command Engine (ICE)

The appendix includes the following topics:

- Introducing ICE
- Integrating a new function
- Creating an ICE template
- Applying ICE message options

Introducing ICE

The Integrated Command Engine (ICE) in the Dynamic Assessment policy adds client/server-based functions. The executable programs and scripts that you integrate through ICE template directives function as security checks.

Use ICE options to:

- Enable and disable ICE templates.
- Enable and disable the messages that identify missing scripts and unmapped messages for debugging purposes.
- Enable and disable messages that are mapped to the output of integrated executables and scripts in ICE templates.

ICE templates integrate user provided programs or scripts into Symantec ESM and map their output to security messages. The templates apply cross-platform using the platform designations specified in ICE template OS/Rev sublists.

Symantec ESM does not provide ICE templates. You must create your own.

See “Creating an ICE template” on page 269.

Integrating a new function

The *Symantec ESM Integrated Command Engine (ICE) Module Training Guide* provides exercises that demonstrate how to:

- Integrate the Netstat command on UNIX and Windows computers
- Integrate the NTODrv utility on Windows computers
- Integrate the PSLogList utility on Windows computers

You can download the Training Guide with the current Security Update release from the Symantec Web site at http://securityresponse.symantec.com/.

To integrate a new function using ICE

1. Create or obtain a script or executable program that runs a query, executes a program, or performs another security assessment function that you want to integrate.
2. Verify the operation of the executable or script before you add it to ICE.
3. Copy the executable or script into a subdirectory on the test agent for ICE executables and scripts.
4. Create an ICE template.
   The ICE template tells where to find the script or executable and how to map its output to ICE messages.
   See "To create an ICE template" on page 269.
5. Add ICE to a demonstration policy in the console.
   See "To add a new policy" on page 30.
6. Enable the template in the Command Engine Templates option.
7. Select applicable ICE options in your demo policy, including options that report missing scripts and unmapped messages for debugging purposes.
8. Enable messages that are mapped in the ICE template to the integrated executables or scripts, and disable all ICE messages that are not appropriate to the integrated executables or scripts.
9. Run the demo policy on a test agent and verify that expected output from the integrated executables or scripts is reported as ICE messages.
   See "To run a policy" on page 33.
10. Disable ICE options that report debugging messages after testing verifies a successful integration, and deploy the module to other agents.

Creating an ICE template

Create an ICE template for each set of related functions.

To create an ICE template

1. In the Symantec ESM console tree, right-click **Templates**, then click **New**.
2. Select **Integrated Command Engine -all**.
3. Type a name for the template. Symantec ESM will add the .ice extension.
4. Click **OK**.
5. In the Template Editor, add one or more of the following records:
   - OS/Release (see “To add an OS/Release record” on page 269).
   - Base Path (see “To add a Base Path record” on page 269).
   - Script Entry (see “To add a Script Entry record” on page 270).
   - Message Maps (see “To add an entry to a OS/Rev sublist” on page 272).
6. Click **Save** and then **Close**.

To add an OS/Release record

1. In the Template Editor, click **Add Row**.
2. In the new template record, click the Name field, then select **OS/Release**.
3. In the Script ID -or- Base Path, Script Name, and Script Parameters fields, delete <NEW>.
4. Add one or more OS/Rev sublist entries (see “To add an entry to a OS/Rev sublist” on page 272).
5. Click **Save**.

To add a Base Path record

1. In the Template Editor, click **Add Row**.
2. Click the Name field of the new template record, then select **Base Path**.
3. In the Script ID -or- Base Path field, replace <NEW> with the path to the directory that contains the executables or scripts that you want to run. The path must be in the ESM directory on an agent.

   For example, to specify the path to a subdirectory named scripts in the ESM directory on a UNIX agent, type **scripts** in the Script ID -or- Base Path field. The module will look for the subdirectory at /esm/scripts.

   On a UNIX agent the scripts Base Path entry points to /esm/. On a Windows agent, the entry points to \Program Files\Symantec\ESM\.

4 Delete <NEW> from the Script Name and Script Parameters fields.

5 Click **Save**.
To add another entry, repeat steps 1-5.

6 Click **Close**.

To add a Script Entry record

1 In the Template Editor, click **Add Row**.

2 Click the Name field of the new template record, then select **Script Entry**.

3 In the Script ID -or- Base Path field, replace <NEW> with a script ID for the function of the executable or script.
This ID appears in the Name field of the console grid when the module reports the output of integrated executables or scripts.

4 In the Script Name field, replace <NEW> with the name of the executable or script.
ICE looks for the executable or script name in the ESM directory that is identified in the template's Base Path record. See "To add a Base Path record" on page 269.

5 In the Script Parameters field, replace <NEW> with the parameters of the executable or script. If there are no parameters, delete <NEW>.

6 Add one or more entries to the following sublists:

- OS/Rev (see "To add an entry to a OS/Rev sublist" on page 272).
- Message Maps (see "To add an entry to a Message Maps sublist" on page 271).

7 Click **Save**.
To add another entry, repeat steps 1-7.

8 Click **Close**.

Note: Do not put internationalized characters or semi-colons (;) in template fields Script Name For Script Entry or Script Parameters For Script Entry.

To add a Message Maps record

1 In the Template Editor, click **Add Row**.

2 Click the Name field of the new template record, then select **Message Maps**.

3 Delete <NEW> from the Script ID -or- Base Path, Script Name, and Script Parameters fields. The fields must be blank.

4. Add one or more Message Maps sublist entries. See "To add an entry to a Message Maps sublist" on page 271.
5. Click **Save**.
   To add another record, repeat steps 1-5.
6. Click **Close**.

To add an entry to a Message Maps sublist

1. In the Template Editor click the Message Maps field. The Message Maps field displays the number of entries in the Message Maps sublist. Initially, the number is 0.
2. In the Message Maps Sublist Editor, click **Add Row.**
3. In the new sublist record, click the Message field, then select the message that you want to map:

Value	Security level
Passed	Green
Failed	Yellow
Informational	Green
Not Applicable	Green
Not Available	Green
User #1/0 User #2/0 User #3/0	Green
User #1/1 User #2/1 User #3/1	Yellow
User #1/2 User #2/2 User #3/2	Yellow
User #1/3 User #2/3 User #3/3	Yellow

Value	Security level
User #1/4	Red
User #2/4	
User #3/4	

4. In the Map String field, replace <NEW> with the character string for the output line that you are mapping. Type the string exactly as it appears in the output line. Message Maps sublist entries are case sensitive.
5. Click the Location field, then select one of the following values:
   - **Starts with**
   - **Contains**
   - **Ends with**

   This value tells ICE where the Map String is located in the output lines you are mapping to the selected message value.
6. Click **Apply**.
   To add another entry, repeat steps 1-6.
7. Click **Close**.

To add an entry to a OS/Rev sublist

1. In the Template Editor, click the OS/Rev field on the template record that you are editing. The field displays the number of entries in the OS/Rev sublist. Initially the number is 0.
2. In the OS/Rev Sublist Editor, click **Add Row**.
3. In the Exclude field, do one of the following:
   - Select the check box to exclude the specified OS and Revision from the executable or script.
   - Clear the check box to include the specified OS and Revision.

   The following table shows where the executable or script runs when the Exclude check box is cleared.

OS setting	Executable or script runs
ALL (or blank)	On all agents.
<Operating system>	Only on agents that have the specified operating system.
<Operating system> + one or more settings in the Release/Revision field	Only on agents that have the specified operating system, releases, and revisions.

The following table shows where the executable or script does not run when the Exclude check box is checked.

OS setting	Executable or script does not run on
ALL (or blank)	Any agent
<Operating system>	Any agent that has the specified operating system.
<Operating system> + one or more settings in the Release/Revision field	Any agent that has the specified operating system, releases, and revisions.

4 Click the OS field, then select an option.

5 In the Release/Revision field, replace <NEW> with a revision ID using the following conventions:

Option	Description
2.5	Only the specified revision.
-2.5	A revision ID with a leading minus (-) sign: the specified revision and all previous revisions.
+2.5	A revision ID with a leading plus (+) sign: the specified revision and all later revisions.

6 Click **Apply**
To add another entry, repeat steps 2-6.

7 Click **Close**.

To remove a record or sublist entry

1 In the Template Editor, click the number of the record that you want to remove, or in a Sublist Editor, the number of the entry. This number is in the leftmost column.
To select a range of records or entries, hold down the Shift key while you click the first and last row numbers in the range.
To select non-sequential records or entries, hold down the Ctrl key while you click the row numbers.

2 In the Template Editor, click **Remove Entry(s)**, or in the Template Sublist Editor, click **Remove list entry** or **Remove list entry(s)**.

3 Click **Apply**.

Applying ICE message options

Any check in ICE can return the messages listed in the table below.

ICE returns the No problems found message when the module cannot execute because required Base Path or Script Entry records are missing from your ICE templates.

To identify any missing scripts, select the ICE Script Missing messages option the first time you run a new executable or script through ICE.

Other common ICE messages indicate problems with ICE templates or problems with the executables or scripts that are defined in ICE templates.

Message name	Title	Class
HEADER	No problems found	0
ILLEGALPATHINSCRIPT	Illegal path in script	0
ILLEGALBASEPATH	Illegal base path	0
SCRIPTERROR	Script error	1

The Integrated Command Engine (ICE) includes the following options:

- Script Missing messages
- Unmapped messages
- Report all stderr messages
- Redirect stderr to stdout
- Return code
- Passed messages
- Failed messages
- Not Applicable messages
- Not Available messages
- User messages

The descriptions below include steps to demonstrate how each option works. These procedures use a demo policy that you need to create.

Script Missing messages

Enable this option to debug a newly-created ICE template before you rely on the messages generated by the template when ICE runs. When a script or executable that is defined in a Script Entry record cannot be located in the Base Path record, the green level Script Missing message is displayed. See "To add a Script Entry record" on page 270 and "To add a Base Path record" on page 269.

This option returns the following message:

Message name	Title	Class
SCRIPTMISSING	Script Missing	0

When this option is disabled, and specified executables or scripts cannot be located, the green level message, No problems found, is displayed.

To demonstrate the option's function

1. Create an ICE template with Base Path and Script Entry records that point to a directory and executable file in the ESM directory structure. See "To create an ICE template" on page 269, "To add a Base Path record" on page 269, and "To add a Script Entry record" on page 270.
   Ensure that no OS/Rev sublist entry excludes the test agent computer.
2. Remove the test executable from its directory.
3. In ICE, enable the Command Engine Templates option.
4. Enable the ICE template.
5. Enable the Script Missing messages option.
6. Run the demo policy on the agent computer.
7. In the console grid, verify that the policy run reports the Script Missing message.

If the correct message is not reported, Ensure that

- Directories and executable files or scripts that are named in ICE template Base Path and Script Entry records exist in the Symantec ESM directory structure on supported agents.
- Directory and file names are spelled correctly in template records.
- The Script Missing messages option is enabled.

Unmapped messages

Enable this option, then run ICE to debug a newly-created template before you rely on the template message mappings. It reports a yellow level Unmapped message for each line of output that is not mapped to an ICE message by a Message Map sublist entry.

The option returns the following message:

Message name	Title	Class
UNMAPPED	Unmapped Message	1

To demonstrate the option's function

1. Create an ICE template that includes a Message Maps sublist that omits at least one mapping to at least one output line from the executable or script. (Message Maps sublists are used in Base Path and Script Entry records.) See "To create an ICE template" on page 269.
   Ensure that no OS/Rev sublist entry excludes the test agent computer.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Enable the Unmapped messages option.
5. Run the demo policy.
6. In the console grid, verify that the policy run reports each unmapped output line with the Unmapped message title.

If the correct message is not reported, Ensure that:

- Message Map sublist entries map all useful and informative output by executables or scripts.
- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.
- The Unmapped messages option is enabled.

Message Maps sublist

Message Maps sublist entries specify how to report the output of executables and scripts that are defined in the ICE template.

Entries in Message Maps sublists contain information needed to map the output of integrated executables or scripts to ICE messages. After you run the module, these messages are displayed in the console grid with distinctive titles and green, yellow, or red security levels.

Record	Entry maps	Notes
Script Entry	Only the executable or script that is specified on the same row as the sublist.	Takes over entries in Message Maps records. Entries are only processed with entries of a Message Maps record.
Message Maps	All executables and scripts that are specified in the template that contains the Message Maps record.	Maps different lines of output with specified character strings to a different ICE message. Entries are processed as a single list.

When you enable the Unmapped messages option, output that is not mapped in Message Maps or Script Entry records is reported as a yellow-level Unmapped Message.

Report all stderr messages

This option enables reporting of all standard error (stderr) messages. Standard error messages are reported from the script.

This option returns the following message:

Message name	Title	Class
STDERRMSG	Stderr message	0

Redirect stderr to stdout

This option enables mapping standard errors (stderr) to defined Message Maps. This option overrides Report all stderr messages and reports all messages that are defined in the Message Maps.

Return code

This option enables checking the return code generated from defined scripts.

This option returns the following message:

Message name	Title	Class
RETCODE	Return code does not match	0

This message is displayed when the return code from the script does not match the given return code.

Passed messages

This option reports output from defined executables or scripts that is mapped to green-level Passed messages in Message Maps sublist entries.

The option returns the following message:

Message name	Title	Class
PASSED	User test passed	0

If you disable this option, the Passed message is not reported.

To demonstrate the option's function

1. Create an ICE template with at least one Message Maps sublist entry that maps an output line from an executable program to the Passed message value. See "To create an ICE template" on page 269, "To add an entry to a Message Maps sublist" on page 271, and "To remove a record or sublist entry" on page 273
   Ensure that no OS/Rev sublist entry excludes the test agent computer.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Ensure that the Passed messages option is enabled.
5. Run the demo policy on an agent computer.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Passed messages.

If the correct message is not reported, Ensure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Failed messages

This option reports output from defined executables or scripts that is mapped to yellow-level Failed messages in Message Maps sublist entries.

The option returns the following message:

Message name	Title	Class
FAILED	Test failed	1

If you disable this option, the Failed message is not reported.

To demonstrate the option's function

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an output line from an executable program to the Failed message value. See "To create an ICE template" on page 269 and "To add an entry to a Message Maps sublist" on page 271.
   Ensure that no OS/Rev sublist entry excludes the test agent computer.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Ensure that the Failed messages option is enabled.
5. Run the demo policy.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Failed messages.

If the correct message is not reported, Ensure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Information messages

This option reports output from specified executables or scripts that is mapped to green-level Information messages in the Message Maps sublist.

The option returns the following message:

Message name	Title	Class
INFORMATIONAL	User test information	0

If you disable this option, the Informational message is not reported.

To demonstrate the option's function

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an output line from an executable program to the Informational message value. See "To create an ICE template" on page 269 and "To add an entry to a Message Maps sublist" on page 271.
   Ensure that no OS/Rev sublist entry excludes the test agent computer.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Ensure that the Information messages option is enabled.
5. Run the demo policy.
6. In the console grid, verify that the policy run reports all output lines that are mapped to Information messages.

If the correct message is not reported, Ensure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Not Applicable messages

This option reports output from defined executables or scripts that is mapped to green-level Not Applicable messages in Message Maps sublist entries.

The option returns the following message:

Message name	Title	Class
NOT APPLICABLE	User test not applicable	0

If you disable this option, the Not Applicable message is not reported.

To demonstrate the option's function

1. Create an ICE template that includes at least one Message Maps sublist entry that maps an executable's or script's output to the Not Applicable message value. See "To create an ICE template" on page 269 and "To add an entry to a Message Maps sublist" on page 271.
   Ensure that no OS/Rev sublist entry excludes the test agent computer.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Ensure that the Not Applicable messages option is enabled.

5 Run the demo policy.

6 In the console grid, verify that all output lines that are mapped to Not Applicable messages are reported.

If the correct message is not reported, Ensure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Not Available messages

This option reports output from specified executables or scripts that is mapped to green-level Not Available messages in the Message Maps sublist.

The option returns the following message:

Message name	Title	Class
NOT AVAILABLE	User test not available	0

If you disable this option, the Not Available message is not reported.

To demonstrate the option's function

1 Create an ICE template that includes at least one Message Maps sublist entry that maps an output line from an executable program to the Not Available message value. See "To create an ICE template" on page 269 and "To add an entry to a Message Maps sublist" on page 271.
Ensure that no OS/Rev sublist entry excludes the test agent computer.

2 In ICE, select the Command Engine Templates option.

3 Enable the ICE template.

4 Ensure that the Not Available messages option is enabled.

5 Run the demo policy.

6 In the console grid, verify that the policy run reports all output lines that are mapped to Not Available messages.

If the correct message is not reported, Ensure that

- In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

User messages

The User messages options report output lines from defined executables or scripts that are mapped to User messages in Message Maps sublist entries.

These options return the following messages:

ICE option	Message name	Title	Class
User #1/0 messages	USER_1_0	User defined #1 w/value of 0	0
User #2/0 messages	USER_2_0	User defined #2 w/value of 0	0
User #3/0 messages	USER_3_0	User defined #3 w/value of 0	0
User #1/1 messages	USER_1_1	User defined #1 w/value of 1	1
User #2/1 messages	USER_2_1	User defined #2 w/value of 1	1
User #3/1 messages	USER_3_1	User defined #3 w/value of 1	1
User #1/2 messages	USER_1_2	User defined #1 w/value of 2	2
User #2/2 messages	USER_2_2	User defined #2 w/value of 2	2
User #3/2 messages	USER_3_2	User defined #3 w/value of 2	2
User #1/3 messages	USER_1_3	User defined #1 w/value of 3	3
User #2/3 messages	USER_2_3	User defined #2 w/value of 3	3
User #3/3 messages	USER_3_3	User defined #3 w/value of 3	3
User #1/4 messages	USER_1_4	User defined #1 w/value of 4	4
User #2/4 messages	USER_2_4	User defined #2 w/value of 4	4
User #3/4 messages	USER_3_4	User defined #3 w/value of 4	4

If you disable an option, its message is not reported.

To demonstrate the options that enable User messages

1. Create an ICE template with Message Maps sublist entries that map output lines from specified scripts or executables to User message values. See “To create an ICE template” on page 269 and “To add an entry to a Message Maps sublist” on page 271.
   Ensure that no OS/Rev sublists entry excludes the test agent computer.
2. In ICE, select the Command Engine Templates option.
3. Enable the ICE template.
4. Ensure that all User message options are enabled.

5 Run the demonstration policy.

6 In the console grid, verify that the policy run reports all output lines are mapped to User messages

If the correct message is not reported, Ensure that

◆ In the Message Maps sublist, map string values are spelled correctly and Location values are accurate.

Index

Symbols

.m files
- .class directive 43
- .customized directive 44
- .module directive 44
- .text directive 44
- .title directive 43
- directives 43
- locations 43
- title directive 43

A

Access computer from network
- Account Integrity module 69

access tokens, creating 75

Account Information checks
- Disabled accounts 48
- Expired accounts 49
- File/folder access for accounts 50
- Locked out accounts 47
- Security groups and their users 45
- Share permissions 52
- User information 49
- User rights for accounts 46
- Users and their security groups 46
- Users with administrator privilege 47

Account Information options
- File/folder access (cont'd) 51
- User information (cont'd) 50

Account Integrity checks
- Access computer from network 69
- Accounts must be disabled 62
- Accounts that never expire 60
- Accounts without time restrictions 58
- Accounts without workstation restrictions 59
- Act as operating system 70
- Add workstations 71
- Adjust memory quotas for a process 71
- Allow logon through Terminal Services 72
- Backup files and directories 72
- Bypass traverse checking 73
- Change system time 74
- Changed groups 67
- Changed users 64
- Create a pagefile 74
- Create a token object 75
- Create permanent shared object 75
- Debug programs 76
- Deleted groups 67
- Deleted users 64
- Deny access to computer from network 76
- Deny logon as a service 78
- Deny logon as batch 77
- Deny logon locally 78
- Deny logon through Terminal Service 79
- Disabled/expired/locked accounts 61
- Enable computer and user accounts for delegation delegation 79
- Excessive number of accounts 60
- Force remote shutdown 80
- Full name and description required 54, 55
- Full/Display name and description 54
- Generate security audits 81
- Groups guest belongs to 57
- Increase quotas 81
- Increase scheduling priority 82
- Load/unload device drivers 82
- Lock page in memory 83
- Log on as a batch job 83
- Log on as a service 84
- Log on locally 85
- Manage audit and security log 85
- Modify firmware values 86
- New groups 66
- New users 63
- Perform volume maintenance tasks 86
- Profile single process 87
- Profile system performance 88
- Remove computer from docking station 88
- Rename administrator account 55
- Rename guest account 56
- Replace process level token 89
- Restore files and directories 89

Shut down the system 90
Synchronize directory service data 90
Take ownership of files or objects 91
Account Integrity header
User rights checks header 69
Account Integrity module 53-92
Account Integrity option
Users to check 53
Account lockout duration
Login Parameters module 155
Account lockout threshold
Login Parameters module 153
accounts 89
Account Information module 45
administrator 55
assigned to security groups 45
autologon disabled 161
deleted 64
disabled 48
disabled, expired, and locked 61
disconnect when hours expire 158
excessive number 60
expired 49
full name and description 54, 55
full/display name and description 54
guest, groups 57
guest, rename 56
inactive 161
local 192
local system 245
locked out 47
lockout counter reset time 156
lockout duration 155
lockout threshold 153
must be disabled 62
never expire 60
new 63
policy settings 49
privileged 134
RAS callback number 177
RAS callbacks required 176
rights 46
RRAS callbacks 175
running services 246
share permissions, directories and printers 167
share permissions, files and folders 52
trusted 79
with administrator privilege 47
without password 206
without time restrictions 58
without workstation restrictions 59
Accounts must be disabled
Account Integrity module 62
Accounts that never expire
Account Integrity module 60
Accounts without passwords
Password Strength module 206
Accounts without time restrictions
Account Integrity module 58
Accounts without workstation restrictions
Account Integrity module 59
ACL control
persistent 191
ACL entries
auditing 236
files 129
registry key permissions 236
remote 250
ACL sublist
Registry template 225
ACL user/group not on system 134
Act as operating system
Account Integrity module 70
Act as operating system,
Account Integrity module 70
Active Directory checks
Computers with applied GPOs 92
Computers without applied GPOs 93
Security groups with applied GPOs 94
Security groups without applied GPOs 94
Users with applied GPOs 93
Users without applied GPOs 93
Active Directory module 92, 92-94
Active Directory objects ownership 91
Add workstations to domain
Account Integrity module 71
Adjust memory quotas for a process
Account Integrity module 71
administrator account, renaming 55
administrator privileges
arranging objects 53
auditing management 85
correcting agent settings 42
creating containers 53
creating pagefile 74
debugging 76
disabling File > Run 259

increasing quotas 81
installation 26
loading/unloading device drivers 82
logging on as a batch job 83
modifying system environment variables 86
profiling single processes 87
profiling system performance 88
restoring files and directories 89
shutting down the system 90
synchronizing directory service data 91
unlocking locked out accounts 155
users with 47
volume maintenance 87
Administrators security group
members 47
shared system folders 165
Adore worm 147
ADS see Active Directory module
agents, correcting 42
Allow any privileged account
File Attributes option 134
Allow logon through Terminal Services
Account Integrity module 72
Anonymous LanMan access disabled
Network Integrity module 168
ANONYMOUS LOGON security group
remote registry access 248
auditing
ACL not checked 236
days to overwrite 258
disk quota exceeded 106
disk quota warning exceeded 107
failed events 255
generate log entries 81
manage 85
overwrite security log 256
RAS 182
RAS NetBIOS 181
security log halts 256
security log size 257
successful events 254
Auditing ACL sublist
File template 120
Auditing sublist
Registry template 231
authentication
plain text 171
RAS retries 180
RAS time limit 181
See also Password Strength checks and passwords 171
Autologon disabled
Login Parameters module 161

B

Back up files and directories
Account Integrity module 72
Backup Integrity check
Backups needed 95
Backup Integrity module 95-96
Backup Integrity options
Folders excluded 96
backup operators
restoring files and directories 89
shutting down the system 90
Backups needed
Backup Integrity module 95
Bad logon counter reset
Login Parameters module 156
batch jobs
deny logon 77
logon 83
Bypass traverse checking
Account Integrity module 73

C

callback number required
RAS requires preset number 177
RRAS preset numbers 177
callbacks required
RAS 176
RRAS 175
CERIAS security information 145, 204
CERT coordination center 145
OS Patches module 204
Change system time
Account Integrity module 74
Changed file (signature)
File Attributes module 128
Changed file (size)
File attributes module 127
Changed file (times)
File Attributes module 126
Changed files (ownership)
File Watch module 139

Changed files (signature)
  File Watch module 139
Changed groups
  Account Integrity module 67
Changed key (time)
  Registry module 238
Changed services
  Startup Files module 243
Changed users
  Account Integrity module 64
Changed value (signature)
  Registry module 239
Changed value (size)
  Registry module 238
check boxes in templates 39
Check Values sublist
  Key and value existence 236
  Registry template 227
checks See security checks
CIAC security information 145, 204
common messages
  File Attributes module 113
  File Watch module 135
  ICE module 274
  OS Patches module 193
  Registry module 220
Common program groups
  User Files module 261
comparison operators 197
Computers with applied GPOs
  Active Directory module 92
Computers without applied GPOs
  Active Directory module 93
Conditions sublist
  comparison operators 197
  Patch template 196
connection errors 28
context menus in templates 39
correctable messages 42
CRC signature changes
  from File Signatures 139
  from snapshot 128
Create a pagefile
  Account Integrity module 74
Create a token object
  Account Integrity module 75
Create permanent shared object
  Account Integrity module 75

D

Data Existence sublist
  Registry template 229
Days until events overwritten
  System Auditing module 258
Debug programs
  Account Integrity module 76
debugging 76
delegation 79
Deleted groups
  Account Integrity module 67
Deleted listening TCP ports
  Network Integrity module 186
Deleted listening UDP ports
  Network Integrity module 190
Deleted network shares
  Network Integrity module 188
Deleted services
  Startup Files module 244
Deleted users
  Account Integrity module 64
demo policy 33
demonstration policy
  ICE module 268
Deny access to this computer from the network
  Account Integrity module 76
Deny logon as a service
  Account Integrity module 78
Deny logon as batch
  Account Integrity module 77
Deny logon locally
  Account Integrity module 78
Deny logon through Terminal Service
  Account Integrity module 79
device drivers 82
dictionary word files 209
directives 43
directories
  restore 89
  shared 167
  synchronize service data 90
  watch 136
Disable Patch module
  OS Patches module 203
Disable patch module
  OS Patch option 193
Disable Run on File menu
  User files module 259

Disable Saved/Never Save
    User Files module 260
Disabled accounts
    Account Information module 48
disabled accounts
    must be 62
Disabled/expired/locked accounts
    Account Integrity module 61
Disallowed services
    Startup Files module 241
disconnect, forced 158
Discovery checks
    Symantec ESM device status 97
    Symantec Intruder Alert device status 99
Discovery module 96-101
Discovery options
    Profile candidate devices 100
    Profile timeout 101
    Report if found 100
    Scan non-responding addresses 101
    Targets 96
Disk Quota checks
    User exceeds quota 108
    User exceeds warning 109
    User quota not enforced 107
    Volume quota disabled 103
    Volume quota enforced 104
    Volume quota exceeds limit 105
    Volume quota not enforced 103
    Volume quota not logged 106
    Volume quota not supported 102
    Volume warning exceeds limit 105
    Volume warning not logged 107
Do not notify ACL not on system
    File Attributes option 134
Do not notify permissions increased
    File Attributes options 134
docking station 88
domains
    adding workstations 71
    trusted 163
Double occurrences option
    Password Strength module 213
drivers, load and unload rights 82
drives, backup needed 95

E

e-commerce malicious files 146
e-finance/banking malicious files 146
EFS not supported
    Encrypted File System module 110
Enable computer and accounts to be trusted for delegation
    Account Integrity module 79
Enabled/Disabled files 35
Enabled/Disabled word files 35
Encrypted File System checks
    EFS not supported 110
    File recovery agents not authorized 112
    Files can be decrypted by others 111
    Percentage of encrypted files 111
Encrypted File System module 110
encryption
    data, RAS 183
    decryption by others 111
    LAN Manager 188
    password, RAS 179
    percentage of files 111
    Syskey 219
environment variables
    firmware 86
    Registry template 227
Everyone security group
    Full Control 133
    members 45
    shared folders 165
    winreg 250
Excessive number of accounts
    Account Integrity module 60
Excludes sublist
    File Watch template 138
existing keys do not exist 236
Expired accounts
    Account Information module 49
expired accounts
    disabled, expired, and locked 61
    never expire 60
    number of days 61
    on domain controllers 49
Expired logon hours disconnect
    Login Parameters module 158

F

failed messages
  ICE module 279
failure audit events 255
FAT partitions
  share permissions 167
  shared folders 164
File ACL
  File Attributes module 129
File and folder permissions
  File Attributes module 132
File attributes
  File Attributes module 125
File Attributes checks
  Changed file (signature) 128
  Changed file (size) 127
  Changed file (times) 126
  File ACL 129
  File and folder permissions 132
  File attributes 125
  File ownership 123
  Files giving all users Full Control 133
  Hidden files and folders 131
  Keywords list 121
File Attributes common messages 113
File Attributes module 113-134
File Attributes options
  Allow any privileged account 134
  Do not notify ACL not on system 134
  Do not notify increased permissions 134
File Attributes templates
  File 115-121
  File Keywords 122
file attributes, loading 115
file attributes, loading, manually 116
File dates option
  OS Patches module 202
File Extension sublist
  File Watch template 151
File Keywords template 122
  Keywords list option 121
  path names 114
File ownership
  File Attributes module 123
File recovery agents not authorized
  Encrypted File System 112
File security more restrictive than share
  Network Integrity module 172
file signatures
  changed from File Signatures template 139
  changed from snapshot 128
  invalid (changed from snapshot) 152
  loading to template 115-117
  malicious 145
File Signatures template 141-143
File template 115-121
  add 115
  Auditing ACL sublist 120
  loading attributes of a single file 115
  loading attributes of all files in folder 115
  loading file attributes manually 116
  loading single file attributes 115
  Permissions ACL sublist 118
File Type sublist
  File Watch template 149
  Malicious File Watch template 149
File versions option
  OS Patches options 202
File Watch checks
  Changed files (ownership) 139
  Changed files (signature) 139
  Invalid signature 152
  Malicious files 145
  New files 143
  Removed files 144
File Watch messages
  common 135
File Watch module 135-153
  Files/directories to watch 136
File Watch template
  editing 136-138
  Excludes sublist 138
  File Extension sublist 151
  File Type sublist 149
  OS/Rev sublist 137
  Signature Patterns sublist 151
  Signature sublist 150
File Watch templates
  File Signatures 141-143
  Malicious File Watch 146-151
File/folder access (cont'd)
  Account Information option 51
File/folder access for accounts
  Account Information module 50

files
  account access 50
  ACL entries 129
  backup needed 95
  changed ownership 139
  changed size 127
  changed time 126
  decryption by others 111
  deleted 144
  Full Control to all users 133
  hidden 131
  new 143
  owner not found 123
  ownership changed 123
  permissions 132
  permissions more restrictive than share 172
  recovery agent 112
  setting permissions 118
  signature changed from snapshot 128
  suspicious 264
  system 264
  take ownership 91
  watch 136
Files can be decrypted by others
  Encrypted File System module 111
Files giving all users Full Control
  File Attributes module 133
files See also shares
Files sublist
  Patch template 196
Files/directories to watch
  File Watch module 136
Files/Folders name lists 35
firmware environment values 86
FIRST security information 145, 204
folders
  account access 50
  changed ownership 139
  deleted 144
  Full Control to all users 133
  hidden 131
  new 143
  permissions 132
  restore 89
  setting permissions 118
  shared 164
  shared, deleted 188
  shared, hidden 168
  shared, modified 187
  shared, new 186
  shared, permissions 167
  watch 136
Folders excluded
  Backup Integrity option 96
Folders sublist
  Malicious File Watch template 149
forbidden keys exist 236
Force remote shutdown
  Account Integrity module 80
Full Control
  Files giving all users Full Control 133
Full name and description required
  Account Integrity module 54, 55
Full/Display name and description
  Account Integrity module 54

G

Generate security audits
  Account Integrity module 81
Generic strings name lists 35
group policy objects
  applied 93
  computers with 92
  computers without 93
  security groups with 94
  security groups without 94
Groups guest belongs to
  Account Integrity module 57
Guest not renamed 56
Guests security group 57

H

Hidden files and folders
  File Attributes module 131
Hidden files and folders,
  File Attributes module 131
Hidden shares
  Network Integrity module 168
Hidden shares,
  Network Integrity module 168
Hide rootkit programs 146
home folder
  changed user 64

Home folder ownership/access
  User Files module 263
home folders
  missing 263
  ownership/access 263

I

ICE module options
  enable failed messages 279
  enable informational messages 279
  enable not applicable messages 280
  enable not available messages 281
  enable user messages 282
ICE module,
  common messages 274
ICE template
  creating 269
  message maps sublists 276
  script entry record 269
Inactive accounts
  Login Parameters module 161
Increase quotas
  Account Integrity module 81
Increase scheduling priority
  Account Integrity module 82
informational messages,
  ICE module 279
InfoSysSec security information 145, 204
installation, Symantec ESM modules 26-28
Installed services
  Startup Files module 240
Integrated Command Engine (ICE) module 32
Internet advisory resources 193
Internet/Network Security security information 146, 204
Invalid signature
  File Watch module 152
IP address ranges 96

K

Key (word) name lists 35
Key and value existence
  Registry module 236
Key name list 35
Key ownership
  Registry module 235
Key permissions
  Registry module 236
key value data size 238
keywords
  File Keywords template 114
Keywords list
  File Attributes module 121
Keywords list option
  File Keywords template 121

L

LAN Manager
  authentication 188
  encryption 188
  hash 211
LanMan authentication
  Network Integrity module 188
Last user hidden
  Login Parameters module 159
Legal notice
  Login Parameters module 157
Lion worm 147
Listening TCP ports
  Network Integrity module 184
Listening UDP ports
  Network Integrity module 184
LiveUpdate frequency check
  Norton AntiVirus 251
  Symantec AntiVirus Corporate Edition 252
Load/unload device drivers
  Account Integrity module 82
Local accounts
  Object Integrity module 192
Local groups
  Network Integrity module 164
local logon
  accounts 85
  deny 78
local system account 245
Lock page in memory
  Account Integrity module 83
locked accounts
  disabled, expired, and locked 61
  reporting 47
Locked out accounts
  Account Information module 47
lockout
  bad logon counter reset 156
  duration 155
  threshold 153

Log on as batch job
- Account Integrity module 83

Log on as service
- Account Integrity module 84

Log on locally
- Account Integrity module 85

Login Parameters checks
- Account lockout duration 155
- Account lockout threshold 153
- Autologon disabled 161
- Bad logon counter reset 156
- Expired logon hours disconnect 158
- Inactive accounts 161
- Last user hidden 159
- Legal notice 157
- Shutdown without logon 160

Login Parameters module 153-162

logon
- as a batch job 83
- as a service 84
- denied as a batch job 77
- denied as a local 78
- denied as a service 78
- deny through Terminal Service 79
- hide previous user name 159
- legal notice 157
- local 85
- name changed 64
- script ownership 261
- script required 265
- through Terminal Services 72

logon hours expired 158

Logon script required
- User Files module 265

M

Malicious File Watch template
- editing 146-151
- File Type sublist 149
- Folders sublist 149
- OS/Rev sublist 148
- Signature sublist 150

Malicious files
- File Watch module 145

Manage audit and security log
- Account Integrity module 85

mandatory keys 236

Maximum password age
- Password Strength module 218

MD4 hashes
- Password Strength module 211

MD5 signature changes
- from File Signatures template 139

MD5 signatures changes
- from snapshot 128

memory
- locked pages 83

memory quotas, increase 71

message maps sublists,
- ICE template 276

messages
- .class directive 43
- correctable 42
- directives 43
- duplicate records 41
- editing 43
- message.dat location 44
- severity 43
- title 43
- updateable 42

messages, common
- File Attributes module 113
- File Watch module 135
- ICE module 274
- OS Patches module 193
- Registry module 220

Microsoft application patches
- OS Patches module 193

Minimum password age
- Password Strength module 218

Minimum password length
- Password Strength module 205

Minimum version check
- Norton AntiVirus 251
- Symantec AntiVirus Corporate Edition 252

missing keys 236

Modified network shares
- Network Integrity module 187

Modify firmware values
- Account Integrity module 86

module options 34

module registration 28

module templates 37

module version numbers 44

modules
- Account Integrity 53-92
- Active Directory 92-94
- Backup Integrity 95-96

Discovery 96-101
Encrypted File System 110
File Attributes 113-134
File Watch 135-153
Integrated Command Engine (ICE) 32
Login Parameters 153-162
Network Integrity 163-190
Object Integrity 191-192
OS Patches 193-203
Password Strength 204-219
Registry 220-239
Response 22, 239
Startup Files 239-250
System Auditing 253-258
User Files 259-266
modules and policies 19

N

name lists
disabling items 211
editing 35
multiple users/groups 36
precedence 36
word files 209
NetBIOS auditing 181
NetBIOS gateway disabled, RAS 179
NetBIOS gateway disabled, RRAS 178
Network Integrity checks
Anonymous LanMan access disabled 168
Deleted listening TCP ports 186
Deleted listening UDP ports 190
Deleted network shares 188
File security more restrictive than share 172
Hidden shares 168
LanMan authentication 188
Listening TCP ports 184
Listening UDP ports 184
Local groups 164
Modified network shares 187
New listening TCP ports 185
New listening UDP ports 189
New network shares 186
Permitted IP protocols 171
Permitted TCP ports 169
Permitted UDP ports 170
Plain text authentication 171
RAS auditing 182
RAS authentication retries 180
RAS authentication time limit 181
RAS enabled 174
RAS encrypted data 183
RAS encrypted password 179
RAS installed 174
RAS NetBIOS auditing 181
RAS NetBIOS gateway disabled 179
RAS requires account callbacks 176
RAS requires preset number 177
RRAS enabled 173
RRAS NetBIOS gateway disabled 178
RRAS requires account callbacks 175
RRAS requires preset number 177
Share permissions 167
Shared folders 164
Shared folders giving all users Full Control 165
Shared printers 166
Trusted domains 163
Network Integrity module 163-190
New files
File Watch module 143
New groups
Account Integrity module 66
New listening TCP ports
Network Integrity module 185
New listening UDP ports
Network Integrity module 189
New network shares
Network Integrity module 186
New services
Startup Files module 244
New users
Account Integrity module 63
Norton AntiVirus LiveUpdate frequency check 251
Norton AntiVirus minimum version check 251
Norton AntiVirus scan frequency check 252
not applicable messages,
ICE module 280
not available messages,
ICE module 281
NT (MD4) hash 211
NTBugtraq security information 146, 204
NTFS partitions
share permissions 167
shared folders 164
NTSecurity Net security information 146, 204

O

Object Integrity checks
- Local accounts 192
- Volumes without ACL control 191

Object Integrity module 191-192

objects
- creating token 75
- permanent shared 75

operators 197

options
- permanently enabled 34
- specifying 34

OS hardening policies 29

OS Patches common messages 193

OS Patches module 193-203
- Disable Patch module 203
- Internet advisory resources 193
- Microsoft application patches 193
- Superseded patches 203

OS Patches options
- Disable patch module 193
- File dates 202
- File versions 202
- Patch Keywords templates 198
- Registry keys 202
- Relaxed 203
- Strict 203
- Template file list 193

OS Patches templates
- Patch Keywords template 198-199
- Patch template 193-198

OS/Rev sublist
- File Watch template 137
- Malicious File Watch template 148

ownership
- accounts 54
- full name and description 54
- home folder 263
- logon scripts 261
- registry key 235
- restore rights 89
- take 91

P

pages, locking in memory 83

Password changes
- Password Strength module 217

Password must expire
- Password Strength module 217

Password Strength checks
- Accounts without passwords 206
- Maximum password age 218
- Minimum password age 218
- Minimum password length 205
- Password changes 217
- Password must expire 217
- Password uniqueness 219
- Password=any username 208
- Password=username 207
- Password=wordlist word 208
- Syskey encryption 219

Password Strength module 204-219
- word files 209

Password Strength options
- Double occurrences 213
- MD4 hashes 211
- Plural forms 214
- Prefix 215
- Reverse order 212
- Suffix 216
- Users to check 205

Password uniqueness
- Password Strength module 219

Password=any username
- Password Strength module 208

Password=username
- Password Strength module 207

Password=wordlist word
- Password Strength module 208

passwords
- RAS encrypted 179
- secure 205
- Security Update installation 26

Patch Keywords template 198-199

Patch Keywords templates option
- OS Patches module 198

Patch module see OS Patches module

Patch template
- Conditions sublist 196
- Files sublist 196
- OS Patches module 193-198
- Superseded sublist 196

path names
- File Keywords template 114

Percentage of encrypted files
- Encrypted File System module 111

Perform volume maintenance tasks
Account Integrity module 86
permanent objects 75
permissions
file and folder 118
registry key 236
shares 167
Permissions ACL sublist
File template 118
Permitted IP protocols
Network Integrity module 171
Permitted TCP ports
Network Integrity module 169
Permitted UDP ports
Network Integrity module 170
phase policies 31
Plain text authentication
Network Integrity module 171
Plural forms option
Password Strength module 214
policies
adding 30
and modules 19
copy between managers 33
create and edit 30
default 31
deleting 31
duplicating 30
editing 30
move between managers 33
OS hardening 29
phase 31
renaming 31
Response 30
sample 31-32
portable computer docking 88
ports
listening, TCP 184
listening, TCP (deleted) 186
listening, TCP (new) 185
listening, UDP 184
listening, UDP (deleted) 190
listening, UDP (new) 189
permitted, TCP 169
permitted, UDP 170
Prefix option
Password Strength module 215
printers See shares
privileged accounts allowed 134
privileged user registry key permissions 236
Procedure Call disabled 247
processes
adjusting memory quotas 71
attack signatures 146
creating access tokens 75
debugging 76
increasing quotas 81
increasing scheduling priority 82
malicious run 145
profiling a single process 87
profiling system performance 88
replacing a process level token 89
Profile candidate devices
Discovery option 100
Profile single process
Account Integrity module 87
Profile system performance
Account Integrity module 88
Profile timeout
Discovery option 101
protocols permitted 171

Q

quotas
increase 81
memory 71
See also Disk Quota

R

RAS auditing
Network Integrity module 182
RAS authentication retries
Network Integrity module 180
RAS authentication time limit
Network Integrity module 181
RAS enabled
Network Integrity module 174
RAS encrypted data
Network Integrity module 183
RAS encrypted password
Network Integrity module 179
RAS installed
Network Integrity module 174
RAS NetBIOS auditing
Network Integrity module 181
RAS NetBIOS gateway disabled
Network Integrity module 179

RAS requires account callbacks
- Network Integrity module 176

RAS requires preset number
- Network Integrity module 177

records, duplicate 41
recovery agents module 112
registry access
- remote 248
- remote by anonymous 248
- remote by non-Administrators 249

Registry checks
- Changed key (time) 238
- Changed value (signature) 239
- Changed value (size) 238
- Key and value existence 236
- Key ownership 235
- Key permissions 236
- Registry value data size 238

registry keys
- changed signature 239
- changed size 238
- changed time 238
- forbidden 236
- mandatory 236
- missing 236
- ownership 235
- permissions 236
- values 227
- winreg 248-250

Registry keys option
- OS Patches module 202

Registry messages, common 220
Registry module 220-239
Registry options
- Template file list 221

Registry template 222-235
- ACL sublist 225
- Auditing sublist 231
- Check Values sublist 227
- Data Existence sublist 229
- Skip Conditions sublist 230
- Snapshot Values sublist 226
- unicode strings 227
- Value Info Queries sublist 228

Registry value data size
- Registry module 238

regular expressions
- required keys 229
- syntax 231-233

Relaxed
- OS Patches module 203

Remote Access Service See RAS
Remote Procedure Call disabled
- Startup Files module 247

Remote registry access (anonymous)
- Startup Files module 248

Remote registry access (non-Administrators)
- Startup Files module 249

Remote registry access permissions
- Startup Files module 248

Remove computer from docking station
- Account Integrity module 88

Removed files
- File Watch module 144

Rename administrator account
- Account Integrity module 55

Rename guest account
- Account Integrity module 56

Replace process level token
- Account Integrity module 89

Report if found
- Discovery option 100

Required services
- Startup Files module 240

requirements, system 25
resource list, Registry template 227
Response module 22, 239
Response policies 30
Restore files and directories
- Account Integrity module 89

Reverse order option
- Password Strength module 212

rootkit programs 147
Routing and Remote Access Service, See RRAS
RPC disabled 247
RRAS enabled
- Network Integrity module 173

RRAS NetBIOS gateway disabled
- Network Integrity module 178

RRAS requires account callbacks
- Network Integrity module 175

RRAS requires preset number
- Network Integrity module 177

S

SACL entry messages 113
sample policies 31-32
SANS security information 146, 204

Scan frequency check
  Norton AntiVirus 252
  Symantec AntiVirus Corporate Edition 253
Scan non-responding addresses
  Discovery option 101
scheduling priorities 82
script entry record
  ICE template 269
Script file extensions option
  User Files module 263
Script ownership/access
  User Files module 261
scripts, logon 265
security checks
  and modules 19
  demonstrate 33
  editing name lists 35
  enable/disable 34
Security event log size
  System Auditing module 257
Security events do not overwrite
  System Auditing module 256
Security events failure auditing,
  System Auditing module 255
Security events success auditing
  System Auditing module 254
security group accounts
  Account Information module 45
  autologon disabled 161
  members 46
  synchronize directory service data 90
  volume maintenance right 86
  with applied GPOs 94
  without applied GPOs 94
security groups
  Administrators 165
  Backup Operators 89
  changed 67
  changed user 64
  deleted 67
  Everyone 57, 165
  Guests 57
  local 164
  members 45
  new 66
  None 57
  user removed 64
Security groups and their users
  Account Information module 45
Security groups with applied GPOs
  Active Directory module 94
Security groups without applied GPOs
  Active Directory module 94
security log
  days to overwrite 258
  halts when full 256
  managing 85
  overwrite when full 256
  size 257
Security Update installation 26-28
SecurityFocus security information 146, 204
services
  changed 243
  deleted 244
  disallowed 241
  installed 240
  listening TCP ports 184
  listening TCP ports, deleted 186
  listening TCP ports, new 185
  listening UDP ports 184
  listening UDP ports, deleted 190
  listening UDP ports, new 189
  logon 84
  new 244
  required 240
  System Event Notification 246
  terminal 79
  unknown 242
  using system account 245
  using user account 246
Services using specified user accounts to run
  Startup Files module 246
Services using system account
  Startup Files module 245
severity 43
Share permissions
  Account Information module 52
  Network Integrity module 167
Shared folders
  Network Integrity module 164
Shared folders giving all users Full Control
  Network Integrity module 165
Shared printers
  Network Integrity module 166
shares
  deleted 188
  folders 164
  folders giving all users Full Control 165

hidden 168
modified 187
new 186
permissions more restrictive than file 172
permissions, reporting 167
printers
Shut down the system
Account Integrity module 90
shutdown
force remote 80
user right 90
without logon 160
Shutdown without logon
Login Parameters module 160
Signature Patterns sublist
File Watch template 151
Signature sublist
File Watch template 150
Malicious File Watch template 150
signatures
changed from snapshot 128, 152
changed registry value 239
loading to File Signatures template 141-143
loading to File template 115-117
malicious 145
Skip Conditions sublist
Registry template 230
snapshot update 42
Snapshot Values sublist
Registry template 226
Startup Files checks
Changed services 243
Deleted services 244
Disallowed services 241
Installed services 240
New services 244
Remote Procedure Call disabled 247
Remote registry access (anonymous) 248
Remote registry access (non-Administrators) 249
Remote registry access permissions 248
Required services 240
Services using specified user accounts to run 246
Services using system account 245
Unknown services 242
Startup Files module 239-250
Storm Center security information 146, 204
Strict option
OS Patches module 203
SU 42
sublist editing 39
Suffix option
Password Strength module 216
Superseded patches
OS Patches module 203
Superseded sublist
Patch template 196
Suspicious files in folder
User Files module 264
Symantec AntiVirus Corporate Edition LiveUpdate frequency check 252
Symantec AntiVirus Corporate Edition minimum version check 252
Symantec AntiVirus Corporate Edition scan frequency check 253
Symantec ESM
candidates 97, 100, 101
running 97
system requirements 25
Symantec ESM device status
Discovery module 97
Symantec Intruder Alert
candidates 99, 100
running 99
Symantec Intruder Alert candidates 101
Symantec Intruder Alert device status
Discovery module 99
Symantec product info checks 250
Symantec security response 145, 204
Synchronize directory service data
Account Integrity module 90
Syskey encryption
Password Strength module 219
system
duplicate files 264
profiling performance 88
requirements 25
shutdown user right 90
shutdown without logon 160
shutdown, remote 80
System Auditing checks
Days until events overwritten 258
Security event log size 257
Security events do not overwrite 256
Security events failure auditing 255

Security events success auditing 254
System halts when log full 256
System Auditing module 253-258
System Event Notification service 246
system folders 165
System halts when log full
System Auditing module 256
system requirements 25
system time 74

T

Take ownership of files or objects
Account Integrity module 91
Targets option
Discovery module 96
TCP ports
deleted 186
listening 184
new listening 185
permitted 169
Symantec ESM 97
Symantec Intruder Alert 99
Template Editor 38
Template file list option
OS Patches module 193
Registry module 221
Template Sublist Editor 39
templates
and modules 37
check box fields 39
context menus 39
creating 37
editing fields 39
editing rows 38
File 115-121
File Keywords 122
File Signatures 141-143
File Watch 136-138
Malicious File Watch 146-151
Patch 193-198
Patch Keywords 198-199
Registry 222-235
update 42
Terminal Service logon
denied 79
Terminal Services logon
allowed 72
time
before bad logon reset 156
disconnect when logon hours expire 158
file times changed 126
maximum wait to end TCP query 101
RAS authentication limit 181
system 74
unrestricted accounts 58
token objects 75
trojan horse programs 146
trusted accounts 79
Trusted domains
Network Integrity module 163
TU 42

U

UDP ports
deleted listening 190
listening 184
new listening 189
permitted 170
unicode strings, Registry template 227
Universal Name Convention 260, 261
Unknown services
Startup Files module 242
update snapshot 42
update template 42
updateable messages 42
User exceeds quota
Disk Quota module 108
User exceeds warning
Disk Quota module 109
User Files checks
Common program groups 261
Disable run on File menu 259
Disable Saved/Never Save 260
Home folder ownership/access 263
Logon script required 265
Script ownership/access 261
Suspicious files in folder 264
User Files module 259-266
User Files options
Script file extensions 263
Users to check 259
User information
Account Information module 49
User information (cont'd) option
Account Information module 50

user messages
  ICE module 282
user name as password 207, 208
user profiles
  common program access 261
  File > Run access 259
  Save settings 260
  script ownership/access 261
User quota not enforced
  Disk Quota module 107
user rights
  granted, removed, revoked 65
user rights checks
  Access computer from network 69
  Accounts that never expire 60
  Accounts without workstation restrictions 59
  Act as operating system 70
  Add workstations to domain 71
  Adjust memory quotas for process 71
  Back up files and directories 72
  Bypass traverse checking 73
  Change system time 74
  Create a pagefile 74
  Create a token object 75
  Create permanent shared objects 75
  Debug programs 76
  demonstrating 69
  Deny access from network 76
  Deny logon as a service 78
  Deny logon as batch 77
  Deny logon locally 78
  Deny logon through Terminal Service 79
  Enable to be trusted 79
  Force shutdown from remote 80
  Full name and description 55
  Full/Display name and description 54
  Generate security audits 81
  Increase quotas 81
  Increase scheduling priority 82
  Load/unload device drivers 82
  Lock page in memory 83
  Log on as a batch job 83
  Log on as a service 84
  Log on locally 85
  Manage auditing and security log 85
  Modify firmware values 86
  Perform volume maintenance tasks 86
  Profile single process 87
  Profile system performance 88
  Remove computer from docking station 88
  Replace process level token 89
  Restore files and directories 89
  Shut down the system 90
  Synchronize directory service data 90
  Take ownership of files or objects 91
  User rights for accounts 46
User rights for accounts
  Account Information module 46
User rights header
  Account Integrity module 69
Users and Groups name list precedence 36
Users and their security groups
  Account Information module 46
Users name lists, editing 35
Users to check option
  Account Integrity module 53
  Password Strength module 205
  User Files module 259
Users with administrator privilege
  Account Information module 47
Users with applied GPOs
  Active Directory module 93
Users without applied GPOs
  Active Directory module 93

V

Value Info Queries sublist
  Registry template 228
Volume quota disabled
  Disk Quota module 103
Volume quota enforced
  Disk Quota module 104
Volume quota exceeds limit
  Disk Quota module 105
Volume quota not enforced
  Disk Quota module 103
Volume quota not logged
  Disk Quota module 106
Volume quota not supported
  Disk Quota module 102
Volume warning exceeds limit
  Disk Quota module 105
Volume warning not logged
  Disk Quota module 107
Volumes without ACL control
  Object Integrity module 191

W

wildcard characters 221
word files 209
  editing 211
  enabling/disabling 211
workstations
  adding to domain 71
  without restrictions 59