

Symantec™ Enterprise
Security Manager™ Security
Update 2008.06.01 (SU 35)
Release Notes



Security Update 2008.06.01 (SU 35) Release Notes

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

Documentation version SU 2008.06.01 (SU 35)

Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, LiveUpdate, Symantec Enterprise Security Architecture, Enterprise Security Manager, and NetRecon are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online 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 and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

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 about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan contractsadmin@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Introducing Security Update 2008.06.01 (SU 35)

This document includes the following topics:

- [What is new in Security Update 2008.06.01](#)
- [About the new operating systems support](#)
- [About the logging feature](#)
- [New checks](#)
- [New messages](#)
- [Modified messages](#)
- [New templates](#)
- [Modified templates](#)
- [Module Enhancements](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)

What is new in Security Update 2008.06.01

The following are new in Security Update (SU) 2008.06.01:

- Support for HP-UX 11.31 on PA-RISC and Itanium
- Support for AIX 6.1 on PPC64

- Support for Windows XP SP3
- Logging feature for the Windows Password Strength module
- 1 new check in the UNIX File Attributes module
- 1 new check in the UNIX Network Integrity module
- 3 new checks in the UNIX Password Strength module
- 4 new checks in the UNIX Startup Files module
- 2 new checks in the UNIX System Queues module
- Enhancements in the UNIX Password Strength and Agent Information modules

Note: On the LiveUpdate wizard, the SU version will now be visible in the following format: SU<YYYY><MM><Release_Version>. Here, YYYY is the year of release, MM is the month of release, and Release_Version is the release version of this SU. For example, SU 2008.06.01 will be displayed as SU2008.06.01 on the LiveUpdate wizard.

About the new operating systems support

SU 2008.06.01 provides support for the following operating systems:

- HP-UX 11.31 on PA-RISC
The existing 6.5.3 HP-UX PA-RISC agent has been certified for HP-UX 11.31 on PA-RISC.
To use this agent, install the existing HP-UX 6.5.3 agent and apply SU 2008.06.01 to it.
- HP-UX 11.31 on Itanium
The existing 6.5.3 HP-UX Itanium agent has been certified for HP-UX 11.31 on Itanium.
To use this agent, install the existing HP-UX 6.5.3 agent and apply SU 2008.06.01 to it.
- AIX 6.1 on PPC64
The existing 6.5.3 AIX PPC64 agent has been certified for AIX 6.1 on PPC64.
To use this agent, install the existing 6.5.3 AIX PPC64 agent and apply SU 2008.06.01 to it.
- Windows XP SP3
The existing 6.5.3 Windows XP agent has been certified for Windows XP SP3.
To use this agent, install the existing 6.5.3 Windows XP agent and apply SU 2008.06.01 to it.

To use these agents, refer to the following Security Response Web site:
<http://www.symantec.com/avcenter/security/Content/2008.02.08.html>

About the logging feature

SU 2008.06.01 introduces a new logging feature that enables ESM to log the information, such as errors and exceptions, that a module generates at the runtime. This feature is currently enabled for the Windows Password Strength module.

About the log levels of the messages

The log level specifies the type and criticality of a message. You can manually create a configuration file and specify the log level of the messages that you want to be logged.

ESM checks the log level that you set in the configuration file and stores only the qualifying messages in the log file.

See “[Creating the configuration file](#)” on page 10.

You can specify the following log levels:

ESMNOLOG	Disable logging for the module
ESMCRITICALFAILURES	All critical failures are logged. ESM always logs all critical failures irrespective of the log level that you specify in the configuration file. However, if ESMNOLOG is specified in the configuration file, ESM does not log the critical failures. ESMCRITICALFAILURES is the default log level and you need not explicitly specify it in the configuration file.
ESMERRORS	All errors are logged. The following are some examples of the errors: <ul style="list-style-type: none">■ Template file not found■ Configuration file not found
ESMEXCEPTIONS	All exceptions are logged.
ESMWARNINGS	All warnings are logged.

ESMINFORMATION	All information messages are logged. The information that is gathered during a policy run is also logged at this level. Note: Enabling this level may affect the performance of the module since all the information messages get logged.
ESMTRACE	All debug information is logged.
ESMPERFMANCETIMING	All time-consuming operations are logged.
ESMAUDIT	All audit information is logged. This level covers the data modification operations such as Correction and Update.
ESMMAXIMUM	Includes all log levels except ESMNOLOG.

You specify the log level in the LogLevel parameter of the configuration file. For example, to log the messages that are related to critical failures, specify the log level as follows:

```
[<module>_LogLevel]= ESMCRITICALFAILURES
```

You can also specify multiple log levels by separating them with a pipe (|) character as follows:

```
[<module>_LogLevel]= ESMCRITICALFAILURES|ESMPERFMANCETIMING
```

You can use log levels for specific operations as follows:

For regular policy runs	ESMCRITICALFAILURES and ESMERRORS
To generate detailed logs for policy failure	ESMCRITICALFAILURES, ESMERRORS, ESMTRACE, and ESMINFORMATION

Creating the configuration file

You can create a configuration file named `esmlog.conf` in the `<esm_install_dir>/config` folder and specify the values that ESM uses to store the logs of a module.

To create the configuration file

- 1 Change to the `<esm_install_dir>/config` folder.
- 2 Create a new text file and specify the parameters and their values.
- 3 Save the text file as `esmlog.conf`.

See [“Parameters of the configuration file”](#) on page 11.

The following is an example of the entries in the configuration file:

[MaxFileSize] = 1024

[NoOfBackupFile] = 20

[LogFileDirectory] = c:\program files\symantec\esm\system\agentname\logs

[password_LogLevel] = ESMINFORMATION|ESMTRACE

[pwdll_LogLevel] = ESMMAXIMUM

Note: No default configuration file is shipped with SU 2008.06.01. You need to manually create the file and specify the parameters in it.

Parameters of the configuration file

[Table 1-1](#) lists the parameters that you need to specify in the configuration file.

Table 1-1 Configuration file parameters

Parameter name	Description	Range of values	Default value
[MaxFileSize]	Specify the maximum file size for the log file in MB	1 MB to 1024 MB (1 GB)	1 MB
[NoOfBackupFile]	Specify the number of backup files of logs that can be stored per module. For example, if the value of NOOFBACKUPFILE is 3, then ESM stores a maximum of 3 backup files for the module.	0 to 20	1
[LogFileDirectory]	Specify the absolute path to store the log file and backup log files.	N/A	The %systemroot%\temp directory is used on the Windows operating systems.

Table 1-1 Configuration file parameters (*continued*)

Parameter name	Description	Range of values	Default value
[<module>_LogLevel]	Specify the log level along with the short name of the module. For example, to log all error messages for the Password Strength module, specify the following: [password_LogLevel]=ESMERRORS	N/A	ESMCRITICALFAILURES (unless ESMNOLOGS is specified)

If the configuration file is not present, ESM considers the default values of all the parameters to store the logs.

About the log file

By default, ESM stores the log file for a module in the temporary directory of the operating system. Separate log files are stored for each module.

The log file has the following format:

<module_name>.log

The <module_name> is the short name of the module. For example, the log file of the Password Strength module is named password.log. The backup file name for password strength module is named password.log_1.bak and so on.

Note: During the process of logging, ESM locks the log file to store the logging information. If the log file is open at that time, the information about the logs might get lost.

Format of the log file

A log file contains the following fields:

Serial Number	Serial number of the log file entry The serial number is displayed in hexadecimal format. The serial number gets reset in the next policy run on the module.
---------------	--

Thread ID	Thread identifier of the process that generated the message
Source File Name	Name of the source file that caused the message to be generated
Line Number	Line number in the source file from where the message was generated
Date	Date on which the log was created
Time	Time at which the log was created
Message	The actual message that was generated along with the log level of that message

About the backup of logs

When the log file reaches a specified size limit, ESM backs up the log file. This size limit is configurable and you can specify it in the `MaxFileSize` parameter of the configuration file.

If the log file reaches the `MaxFileSize` value, ESM creates a backup of the log file depending on the `NoOfBackupFile` value that is specified in configuration file. For example, if the `NoOfBackupFile` value is 0, ESM overwrites the existing log file, if any, for the module.

New checks

New checks have been added in the following modules:

- File Attributes (UNIX)
- Network Integrity (UNIX)
- Password Strength (UNIX)
- Startup Files (UNIX)
- System Queues (UNIX)

File Attributes (UNIX)

The following new check has been added to the File Attributes (UNIX) module:

- Detect Extended attributes

Detect Extended attributes

This check verifies whether the computer contains any files and directories with extended attributes. This check is applicable for Solaris 10 only.

[Table 1-2](#) lists the messages that this check reports.

Table 1-2 Message for the Detect Extended attributes check

Message ID	Message Title	Message Severity
STKU_FILE_EXT_ATTR_SET_R	File has extended attributes set on it	red-4
STKU_FILE_EXT_ATTR_SET_Y	File has extended attributes set on it	yellow-1
STKU_FILE_EXT_ATTR_SET_G	File has extended attributes set on it	green-0

See [“Extended Attributes template \(UNIX File Attributes\)”](#) on page 22.

Network Integrity (UNIX)

The following new check has been added to the Network Integrity (UNIX) module:

- Daemon logging

Daemon logging

This check reports the running daemons whose corresponding logging file is not found on the agent machine. Use the template to specify the daemon name and the logging file for the check to work.

[Table 1-3](#) lists the messages that this check reports.

Table 1-3 Message for the Daemon logging check

Message ID	Message Title	Message Severity
STKU_DAEMON_NOLOG	Daemon logging is not configured	yellow-1

You can use the Daemon Logging check to see whether a daemon is logging in a specific file. For example, if you want to check if the FTP daemon is logging in a specific file, include the FTP daemon name and the logging file name in the Daemon Logging template. You can include multiple entries of the daemon-logging file pairs in the template.

If the daemon is running and the corresponding logging file is not found, ESM reports a violation. If the logging file for a running daemon is present, ESM reports the 'No problems found' message.

If any of the daemon-logging file pairs satisfies the condition, the module ignores the other pairs that are listed in the template, and reports the 'No problems found' message.

You can specify similar information for other daemons that you want to check in the Daemon Logging template. You may create separate templates for the daemons that you want to check.

See [“Daemon Logging template \(UNIX Network Integrity\)”](#) on page 22.

Password Strength (UNIX)

The following new checks have been added to the Password Strength (UNIX) module:

- Verify DICTIIONBBDIR entry
- Verify DICTIIONLIST entry
- NAMECHECK allows username=password

Verify DICTIIONBBDIR entry

DICTIIONBBDIR is a parameter that points to the directory where the dictionary databases reside.

This check verifies if DICTIIONBBDIR refers to the value that is specified in the User Defined Path field of this check. If the user-defined path is not specified, the value of DICTIIONBBDIR parameter mentioned in /etc/default/passwd is considered.

If neither DICTIIONLIST nor DICTIIONBBDIR is specified, the system does not perform a dictionary check on the passwords when they are being set.

This check is available on Solaris 10 only.

[Table 1-4](#) lists the messages that this check reports.

Table 1-4 Messages for the Verify DICTIIONBBDIR entry check

Message Name	Message Title	Message Severity
STKU_NO_DICTIIONBBDIR	Verify DICTIIONBBDIR entry	yellow-1
STKU_NOTSUPPORT_DICTIIONBBDIR	DICTIIONBBDIR not supported	green-0

Verify DICTONLIST entry

DICTONLIST is a parameter that holds a list of comma-separated dictionary file names.

This check verifies if DICTONLIST has been set to /usr/share/lib/dict/words. This check is available on Solaris 10 only.

If neither DICTONLIST nor DICTONDBDIR is specified, the system does not perform a dictionary check on the passwords when they are being set.

[Table 1-5](#) lists the messages that this check reports.

Table 1-5 Messages for the Verify DICTONLIST entry check

Message Name	Message Title	Message Severity
STKU_NO_DICTONLIST	Verify DICTONLIST entry	yellow-1
STKU_NOTSUPPORT_DICTONLIST	DICTONLIST entry not supported	green-0

NAMECHECK allows username=password

This check reports a violation if the NAMECHECK setting allows the users to keep their user name and password the same. This check is available on Solaris 10 only.

[Table 1-6](#) lists the messages that this checks reports.

Table 1-6 Messages for the NAMECHECK allows username=password check

Message Name	Message Title	Message Severity
STKU_NAMECHECK	NAMECHECK allows username=password	yellow-1
STKU_NOTSUPPORT_NAMECHECK	NAMECHECK entry not supported	green-0

Startup Files (UNIX)

The following checks have been added to the Startup Files (UNIX) module:

- Connection logging is not enabled
- Services which are enabled
- Verify Network parameter Values
- Grub password

Connection logging is not enabled

This check reports a violation if connection logging is not enabled for the inetd based services on Solaris 10. This check reports on the default setting of `tcp_trace` and the setting of the individual services that are enabled or online.

If `inetd` is running, the tracing feature can be used to log information about the source of any network connections seen by the daemon.

This check is available on Solaris 10 only.

[Table 1-7](#) lists the messages that this check reports.

Table 1-7 Messages for the Connection logging is not enabled check

Message ID	Message Title	Message Severity
STKU_TRACED_SERVICE	Connection logging is not enabled for this service	yellow-1
STKU_DEF_TRACED_SERVICE	Default inetd Settings Connection logging is not enabled	yellow-1

Services which are enabled

This check lists the enabled services from the template that are recommended to be disabled. This check is available on Solaris 10 only.

[Table 1-8](#) lists the messages that this check reports.

Table 1-8 Messages for the Services which are enabled check

Message ID	Message Title	Message Severity
STKU_ENABLED_SERVICE_Y	This service has been enabled	yellow-1
STKU_ENABLED_SERVICE_R	This service has been enabled	red-4
STKU_ENABLED_SERVICE_G	This service has been enabled	green-0

See “[SVCS Enabled Services template \(UNIX Startup Files\)](#)” on page 24.

Verify Network parameter Values

This check verifies whether the network and the routing parameters have been set according to the recommended values. This check is available on Solaris 10 only.

[Table 1-9](#) lists the message that this check reports.

Table 1-9 Message reported by the Verify Network parameter Values check

Message ID	Message Title	Message Severity
STKU_NW_RT_PARAMETERS	This Network parameter value is not as per recommended	yellow-1

Grub password

This check verifies whether the boot loader password is enabled on the system. This check is available only for the Solaris 10 computers on x86 platform.

[Table 1-10](#) lists the message that this check reports.

Table 1-10 Message reported by the Grub password check

Message ID	Message Title	Message Severity
STKU_BOOTPASSWORD	Grub password	red-4

System queues

The following checks have been added to the System Queues module:

- Only Root access to AT subsystem
- Only Root access to CRON subsystem

Only Root access to AT subsystem

This check verifies whether root is the only user that is allowed to run the `at` command.

[Table 1-11](#) lists the messages that this check reports.

Table 1-11 Messages reported by the Only Root access to AT subsystem check

Message ID	Message Title	Message Severity
STKU_ATSUONLY	Only root can use at and batch	green-0
STKU_ATALLOWWARN	Non root user allowed to use at and batch	red-4
STKU_ATDENYEXISTS	at.deny file exists	red-4
STKU_CRONNSUSER	Non-existent user configured for cron or at	green-0

Only Root access to CRON subsystem

This check verifies whether root is the only user that is allowed to run the `crontab` command.

[Table 1-12](#) lists the messages that this check reports.

Table 1-12 Messages reported by the Only Root access to CRON subsystem check

Message ID	Message Title	Message Severity
STKU_CRONSUONLY	Only root can use crontab	green-0
STKU_CRONALLOWWARN	Non root user allowed to use crontab	red-4
STKU_CRONDENYEXISTS	cron.deny file exists	red-4
STKU_CRONNSUSER	Non-existent user configured for cron or at	green-0

New messages

New messages have been added to the following checks:

- All checks (Windows Group Policy)
- Login requires password (Password Strength)
- NIS/NIS+ enabled (Network Integrity)
- Non-wrapped services (Startup Files)

All checks (Windows Group Policy)

A new message has been added to the all checks in the Group Policy module. This message is reported if the Group policy is not found on the computer.

[Table 1-13](#) lists the new message.

Table 1-13 New message for the System Services check

Message ID	Message Title	Message Severity
ESM_POLICY_NOT_FOUND	Group policy not found on the system	red-4

Login requires password (UNIX Password Strength)

A new message has been added to the Login requires password check in the Password Strength module. This message is reported when the password authentication parameters values are not found. This message is reported on AIX operating systems only.

[Table 1-14](#) lists the new message.

Table 1-14 New message for the Login requires password check

Message ID	Message Title	Message Severity
STKU_PASSREQ_NOTFOUND	Default password authentication parameter values not provided	yellow-1

NIS/NIS+ enabled (UNIX Network Integrity)

A new message has been added to the NIS/NIS+ enabled check in the Network Integrity module for UNIX. This message is reported as a warning when any error occurs while the check retrieves the Network Information Service (NIS) name and the domain name.

[Table 1-15](#) lists the new message:

Table 1-15 New message for the NIS/NIS+ enabled check

Message ID	Message Title	Message Severity
STKU_NIS_NISPLUS_WARN	NIS/NIS+ warning	yellow-1

Non-wrapped services (UNIX Startup Files)

A new message has been added to the Non-wrapped services check in the Startup Files module for Solaris 10. This message is reported when the `tcp_wrappers inetd` service is not set to `TRUE`.

[Table 1-16](#) lists the new message.

Table 1-16 New message for the Non-wrapped services check

Message ID	Message Title	Message Severity
STKU_DEF_NON_WRAPPED_SERVICE	Default Settings for inetd Non-wrapped service	yellow-1

Modified messages

Messages of the following checks have been modified:

- Password in `/etc/passwd` check (UNIX Account Integrity)
- Current directory in startup `PATH` (UNIX Startup Files)

Note: On the old messages, if you applied any suppression involving the Information field of the message, the suppression will no longer be available.

Password in `/etc/passwd` check (UNIX Account Integrity)

The severity of the `STKU_PASSEXISTED` message for the Password in `/etc/passwd` check in the Account Integrity (UNIX) module has been changed to `red-4`.

Current directory in startup `PATH` (UNIX Startup Files)

The Current directory in startup `PATH` check in the Startup Files (UNIX) module now reports separate messages with different information in the Information field for the following conditions of the `PATH` variable:

- `PATH` contains an empty current directory
- `PATH` contains the current directory
- `PATH` contains the trailing colon

New templates

The following new templates have been added in SU 2008.06.01:

- Daemon Logging
- Extended Attributes
- SVCS Enabled Services

Daemon Logging template (UNIX Network Integrity)

The Daemon logging template has been introduced for the Daemon logging check in the Network Integrity (UNIX) module. You can use this template to specify the daemons and their corresponding logging files.

The Daemon logging template has a default .dl extension.

See [“Daemon logging”](#) on page 14.

Creating the Daemon Logging template

You must create and enable a new Daemon Logging template before you run the Daemon Logging check.

To create a Daemon Logging template

- 1 In the tree view, right-click **Templates**, then click **New**.
- 2 In the Create New Template dialog box, select **Daemon Logging - all**.
- 3 Type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .dl extension to the file name.
- 4 Click **OK**.

Using the Daemon Logging template

The Daemon logging template contains the following fields:

Daemon	Specify the daemon name
Logging file	Specify the logging file name for the daemon

Extended Attributes template (UNIX File Attributes)

The Extended Attributes template has been introduced for the Detect extended attributes check in the File Attributes (UNIX) module. You can use this template

to specify the paths for checking the extended attributes that are set on the files and directories in Solaris 10.

The Extended Attributes template has a default .s10 extension.

See “[Detect Extended attributes](#)” on page 14.

Creating the Extended Attributes template

You must create and enable a new Extended Attributes template before you run the Detect extended attributes check.

To create an Extended Attributes template

- 1 In the tree view, right-click **Templates**, then click **New**.
- 2 In the Create New Template dialog box, select **Extended Attributes - Solaris 2.6**.
- 3 Type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .s10 extension to the file name.
- 4 Click **OK**.

Using the Extended Attributes template

The Extended Attributes template contains the following fields:

OS/Rev	<p>Specify the following in this sublist:</p> <ul style="list-style-type: none">■ Exclude Check this check box to exclude this item for the File Attributes checks■ OS Specify the operating system that you want to include in this item■ Release/Revision Specify the version of the operating system that you want to include
Directory/File Name	<p>Specify the name of the file or directory that you want check for extended attributes</p> <p>You must use the wildcard character '*' while specifying the file or the directory name for the option specified in the Item type field to work.</p>

Depth	<p>Specify the level till which ESM can traverse a folder</p> <p>You can select the following values:</p> <ul style="list-style-type: none">■ N: No traversal■ A: Traverse all levels■ 0: Traverse the current level only■ 1: Traverse 1 level deep■ 2: Traverse 2 levels deep■ 3: Traverse 3 levels deep■ 4: Traverse 4 levels deep■ 5: Traverse 5 levels deep■ 6: Traverse 6 levels deep■ 7: Traverse 7 levels deep■ 8: Traverse 8 levels deep■ 9: Traverse 9 levels deep
Item Type	<p>Specify whether you want to report only files, only directories, or files and directories, in this sublist.</p> <p>This sublist contains the following options:</p> <ul style="list-style-type: none">■ Files■ Directories■ Both <p>Both is the default value.</p> <p>You must use the wildcard character '*' while specifying the file or the directory name in the Directory/File Name field for this option to work. If you do not use '*' in the file/directory name, ESM considers Both as the value for this field and scans all files and directories.</p>
Severity	<p>Specify the severity for the messages that ESM will report on this data</p> <p>You can specify one of the following values:</p> <ul style="list-style-type: none">■ Green■ Yellow■ Red

SVCS Enabled Services template (UNIX Startup Files)

The SVCS Enabled Services template has been introduced for the Services which are enabled check in the Startup Files (UNIX) module. You can use this template to specify the services under the svcadm umbrella for Solaris 10.

The SVCS Enabled Services template has a default .vs extension.

See “[Services which are enabled](#)” on page 17.

Creating the SVCS Enabled Services template

You must create and enable a new SVCS Enabled Services template before you run the Services which are enabled check.

To create a SVCS Enabled Services template

- 1 In the tree view, right-click **Templates**, then click **New**.
- 2 In the Create New Template dialog box, select **SVCS Enabled Services - Solaris 2.6**.
- 3 Type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .vs extension to the file name.
- 4 Click **OK**.

Using the SVCS Enabled Services template

The SVCS Enabled Services template contains the following fields:

Services(FMRI)	Specify the FMRI of the service that you want to report on For example, svc:/network/ftp:default.
Severity	Specify the severity for the messages that ESM will report on this data You can specify one of the following values: <ul style="list-style-type: none">■ Green■ Yellow■ Red
Comments	Specify the text that you want to display with messages in the console grid when you run the module

Modified templates

The following templates have been modified:

- DCOM Machine Restriction (Windows Active Directory)
- Password Requirements (UNIX Password Strength)

DCOM Machine Restriction (Windows Active Directory)

A new column named Name has been added to the DCOM Machine Restriction template in the Active Directory module. You can specify the DCOM policy setting in the Name column of the template. This value is displayed in the Name column of the message reported on the console.

Password Requirements (UNIX Password Strength)

A new column named Required has been added to the Password Requirements template for the Password Requirements check in the Password Strength module. You can specify the following values in the Required column:

Mandatory	Specifies that the file containing the password settings must exist.
Optional	Specifies that the file containing the password settings may not exist.
Ignored	Specifies that the file containing the password settings is ignored.

Module Enhancements

The following enhancements have been made in the Agent Information and Password Strength modules:

Agent Information	The Agent version check now reports the exact version information for ESM agents. For example, the module now reports the version as ESM 6.5.3 instead of ESM 6.5 (2007/03/23 03:28).
Password Strength (HP-UX)	The following checks are now supported on HP-UX 11i computers in both trusted and non-trusted modes: <ul style="list-style-type: none">■ Minimum upper case characters■ Minimum lower case characters■ Minimum digits■ Minimum special characters

<p>Password Strength (HP-UX)</p>	<p>The following checks are now supported on HP-UX 11i computers to report system-level settings in the non-trusted mode:</p> <ul style="list-style-type: none"> ■ Minimum password age ■ Maximum password age
----------------------------------	--

Resolved issues

The following issues are resolved in SU 2008.06.01:

<p>Account Information (Windows)</p>	<p>The User information check has been modified to correctly report information about the last password change as follows:</p> <ul style="list-style-type: none"> ■ For the users that have the 'user must change password on next logon' key enabled, the following message is reported: Password last changed: User must change password at next logon
<p>Account Integrity (HP-UX)</p>	<p>Previously, the Password in <code>/etc/passwd</code> check used to expect only the '*' or 'x' values for trusted mode and shadow mode respectively for the root user in the <code>/etc/passwd</code> file. The check used to fail if any other values were specified in the file.</p> <p>The check now correctly reports even if any value other than '*' or 'x' is specified in the <code>/etc/passwd</code> file and reports messages with a Red severity if a user's password is found in the <code>/etc/passwd</code> file.</p> <p>See “Modified messages” on page 21.</p>
<p>File Access (UNIX)</p>	<p>The File Access module no longer reports any messages when none of the following checks is enabled: Read permission, Write permission, and Execute permission.</p>
<p>File Attributes (Windows)</p>	<p>You can now check/uncheck the Enable Auditing ACL check box in the File Attributes template when you add a file/directory to it.</p>

File Find (Solaris)	<p>The description of the SUID/SGID shell escape files check has been modified to the following make the check's functionality clearer:</p> <p>This option modifies the behavior of the Setuid files, Setgid files, Setuid executable files and Setgid executable files checks. When this option and one or all of these security checks are enabled, the checks examine the files that are listed in the agent's /etc/shells file, as well as the shell escape files specified in the file list, for setuid and/or setgid attributes. Enter the full path names in the file list to specify the shell escape files that need to be included in the check. This check is dependent on the Starting directories check.</p>
File System Entitlement (Windows Server 2000)	<p>Previously, the File System Entitlement module was unable to report the permissions on the network share when \\localhost was specified in the File System Entitlement template.</p> <p>The module has been modified and it now reports the permissions on the network share when \\localhost is specified in the template.</p>
File Watch (Windows)	<p>The Malicious files check now reports the "File access blocked" message, instead of an unexpected system error, when it tries to access a locked file.</p>
Group Policy (Windows)	<p>The Group Policy module now reports the following message if the group policy is not found on the system:</p> <p>Group policy not found on the system</p> <p>See "All checks (Windows Group Policy)" on page 20.</p>
Templates of the following modules on VMware ESX server:	<p>In the templates, you can now restrict the Release/Revision field under the OS/Rev sublist to a specific version of VMware ESX server.</p>
<ul style="list-style-type: none"> ■ File Attributes ■ File Find ■ File Watch ■ Integrated Command Engine ■ Password Strength 	<p>To know the version of VMware ESX server, run the following command:</p> <pre>/usr/bin/vmware -v</pre>

Login Parameters (AIX)	<p>The Excessive failed logins for users check now correctly reports the following values in the Information field of the messages for AIX agents:</p> <ul style="list-style-type: none"> ■ User Name of the user ■ Fail Number of failed logon attempts ■ Limit Limit of the failed logons ■ Hours Time duration in hours
Network Integrity (UNIX)	<p>Previously, in case of any errors while retrieving the Network Information Service (NIS) name and the domain name, the module used to report an unexpected system error. The module now reports a warning message instead of an error.</p> <p>See “NIS/NIS+ enabled (UNIX Network Integrity)” on page 20.</p>
Network Integrity (AIX)	<p>The messages reported by the FTP session logging disabled and FTP debug logging disabled checks have been modified to indicate specific information about the remote computer when the FTP daemon is configured for forward logging in the syslog file.</p> <p>The checks now display information as follows in the Information field:</p> <p>Syslog daemon configured to log facility: daemon; priority: info, to @loghost. Though the syntax appears to be correct, due to many other factors, ESM cannot verify this.</p> <p>In this message, @loghost is the remote computer whose entry exists in the syslog configuration file.</p>
Network Integrity (Solaris)	<p>A new check named Daemon logging has been added to the Network Integrity module. This check reports 'No problems found' if any of the running daemons has a corresponding log file that is specified in the template.</p> <p>See “Daemon logging” on page 14.</p>
Password Strength (AIX)	<p>Previously, the Login requires password check used to report incorrectly if the value of the SYSTEM parameter in the /etc/security/user file exceeded 32 characters.</p> <p>The module has been modified and the SYSTEM parameter can now accommodate up to 1024 characters.</p>

Password Strength (Windows)	The Password Strength module no longer reports an unexpected system error while reporting on the domain user names that contain double-byte characters.
Registry (Windows)	You can now check/uncheck the Enable Auditing Checking check box in the Registry template when you add a key to it.
Registry (Windows)	<p>Previously, the Additional ACL entry message used to report 'Unknown account' in the Information field for all accounts that are not present or are removed, and have permissions of registry keys and their subkeys.</p> <p>The module has been modified and it now reports the SID of the unknown account to report unique messages.</p>
Startup Files (Windows)	The Startup Files module now reports the 'No problems found' message, instead of the 'service does not exist' message, when a service that is specified in the template does not exist on the agent.
Startup Files (Solaris 10)	<p>The following checks now correctly reports the services that are enabled or disabled on Solaris 10 operating systems:</p> <ul style="list-style-type: none">■ Installed services■ Changed services■ New services■ Deleted services■ Duplicate services■ Non-wrapped services
LiveUpdate packages (Solaris SPARC)	<p>The SU LiveUpdate packages for ESM 6.0 agents on Solaris SPARC will be shipped with the promiscCollector executable from the SU 2008.06.01 release onwards.</p> <p>The Promiscuous mode check in the Network Integrity module uses the promiscCollector executable to detect the promiscuous mode.</p>
User Files (UNIX)	The Umask (parsing startup scripts) check has been modified to report the umask settings of the users, which have digits in their names, correctly from the .profile file.
User Files (AIX)	The Umask (parsing startup scripts) check has been enhanced to support the inclusion of the /etc/security/user file in the namelist. The /etc/security/user file contains the system-specific and user-specific Umask settings.

Known issues

The following issues are known in SU 2008.06.01:

Group Policy (Windows) The output format of the messages for the following checks has changed:

- Account Policies - Password Policy
- Account Policies - Account Lockout Policy
- Account Policies - Kerberos Policy
- Local Policies - Audit Policy
- Local Policies - Security Options
- Event Log

The following is the new format in which the messages are now displayed in the Information field:

Expected: <value>; Found: <value>

Note: On the old message, if you applied any suppression involving the Information field of the message, the suppression will no longer be available.

Password Strength (Windows Vista/Server 2008)

By default, LAN Manager (LM) hashes is not enabled on Windows Vista/Server 2008 operating systems. As a result, the following checks do not report correctly on these operating systems:

- Password=username
- Password=any username
- Password=wordlist word
- Double occurrences
- Reverse order
- Plural
- Suffix
- Prefix

To resolve this issue, enable LM hashes in your Local Security Policy as follows:

- Click Start > Programs > Administrative Tools > Local Security Policy.
- Click Local Policies and then double-click Security Options.
- Double-click Network security: Do not store LAN Manager hash value on next password change.
- Click Enabled, and then click OK.

Password Strength (Password Requirements template on UNIX) When you upgrade to SU 2008.06.01, the new column named Required in the Password Requirements template does not get updated for the old entries present in the template.

To resolve this issue, delete the existing template and create it again after you apply SU 2008.06.01.

See [“Modified templates”](#) on page 25.

System requirements

Symantec reserves the right to certify the Security Update on the new versions of these operating systems before officially supporting them.

[Table 1-17](#) lists the supported operating systems for SU 2008.06.01.

Table 1-17 Supported operating systems for SU 2008.06.01

Agent operating system	Platform	Supported versions on 6.0	Supported versions on 6.5.x
AIX	RS 6000	N/A	5.2 (32-bit and 64-bit) 5.3 (32-bit only)
AIX	PPC 64	5.3 (64-bit only)	5.3 (64-bit only) 6.1 (64-bit) (supported on 6.5.3 only)
ESX Server	x86, Opteron	N/A	3.0.2 (supported on 6.5.3 only)
HP-UX	PA-RISC	10.20/11.0/11.11	11.0/ 11.11
HP-UX	PA-RISC	N/A	11.23/11.31 (supported on 6.5.3 only)
HP-UX	Itanium®	11.23	11.23 11.31 (supported on 6.5.3 only)
Red Hat Enterprise Linux	IBM z-series (s390x)	N/A	5.x (supported on 6.5.3 only)

Table 1-17 Supported operating systems for SU 2008.06.01 (*continued*)

Agent operating system	Platform	Supported versions on 6.0	Supported versions on 6.5.x
Red Hat Enterprise Linux ES	x86, Opteron and EM64T	3.0	3.0/4.0
Red Hat Enterprise Linux ES	x86, Opteron, EM64T, and IA64	N/A	5.0/5.1
Red Hat Enterprise Linux WS and AS	x86, Opteron and EM64T	3.0	3.0/4.0
Red Hat Enterprise Linux AS	Itanium®	3.0	3.0/4.0
Sun Solaris	SPARC	2.8/2.9/2.10	2.8/2.9/2.10
Sun Solaris	x86, Opteron and EM64T	N/A	2.10
SUSE Linux Standard Server	x86	N/A	9
SUSE Linux Enterprise Server	x86	9	9/10
SUSE Linux Enterprise Server	Itanium®	9	9/10
SUSE Linux Enterprise Server	Opteron and EM64T	N/A	9/10 (supported on 6.5.3/6.5.3 SP1/6.5.3 SP2 only)
SUSE Linux Enterprise Server	IBM PPC e-Server	N/A	9/10
Windows 2000 Professional and Server	x86	All	All
Windows Server 2003	x86	All	All
Windows Server 2003	Itanium®	All	All
Windows Server 2003 Enterprise	Opteron and EM64T	N/A	All

Table 1-17 Supported operating systems for SU 2008.06.01 (*continued*)

Agent operating system	Platform	Supported versions on 6.0	Supported versions on 6.5.x
Windows Vista	x86	N/A	Enterprise and Business editions (Supported on 6.5.2 and later)
Windows Vista	Opteron and EM64T	N/A	Enterprise and Business editions (Supported on 6.5.2 and later)
Windows XP Professional	x86	SP2	SP2 SP3 (supported on 6.5.3 only)
Windows Server 2008	x86	N/A	All (supported on 6.5.3 only)
Windows Server 2008	Opteron and EM64T	N/A	All (supported on 6.5.3 only)
Windows Server 2008	Itanium®	N/A	All (supported on 6.5.3 only)
Windows Server 2008 Core Installation	x86	N/A	All (supported on 6.5.3 only)
Windows Server 2008 Core Installation	Opteron and EM64T	N/A	All (supported on 6.5.3 only)

Table 1-18 lists the post-install disk space usage for an ESM 6.5 agent with SU2008.06.01 applied. The amount of disk space required by each agent depends on its operating system.

Table 1-18 Post-install agent disk space requirements for SU 2008.06.01

Agent operating system	Disk space required (in MB)
AIX /RS 6000	211
AIX (PPC64)	212
HP-UX (PA-RISC)	126

Table 1-18 Post-install agent disk space requirements for SU 2008.06.01
(continued)

Agent operating system	Disk space required (in MB)
HP-UX (Itanium®)	128
Red Hat Enterprise Linux ES (x86)	79
Red Hat Enterprise Linux WS and AS (AMD64)	86
Red Hat Enterprise Linux AS (Itanium®)	109
Red Hat Enterprise Linux WS and AS (EM64T)	90
Red Hat Enterprise Linux on IBM z-series (s390x)	98
Sun Solaris 2.8/2.9 (SPARC)	99
Sun Solaris 10 (SPARC)	103
Sun Solaris 10 (x86, Opteron and EM64T)	75
SUSE Linux Enterprise Server 9 (x86)	75
SUSE Linux Enterprise Server 9 (Itanium®)	94
SUSE Linux Enterprise Server on IBM PPC e-Server	74
SUSE Linux Enterprise Server (Opteron and EM64T)	137
Windows 2000 Professional and Server (x86)	86
Windows Server 2003 (x86)	86
Windows Server 2003 (Itanium®)	149
Windows Server 2003 Enterprise (Opteron and EM64T)	70
Windows XP Professional (x86)	84
Windows Vista (x86)	43
Windows Vista (Opteron and EM64T)	82
Windows Server 2008 (x86)	56
Windows Server 2008 (Itanium®)	140

Table 1-18 Post-install agent disk space requirements for SU 2008.06.01
(continued)

Agent operating system	Disk space required (in MB)
Windows Server 2008 (Opteron and EM64T)	79
Windows Server 2008 Core Installation (x86)	56
Windows Server 2008 Core Installation (Opteron and EM64T)	94