Symantec™ Enterprise Security Manager™ Security Update 2009.09.01 (SU 38) Release Notes

symantec™

Symantec™ Enterprise Security Manager™ Security Update 2009.09.01 (SU 38) Release Notes

Documentation version: SU 2009.09.01

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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	customercare_apac@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.

Symantec ESM Security Update 2009.09.01 (SU 38) Release Notes

This document includes the following topics:

What's new in Security Update 2009.09.01

The following are new in Security Update (SU) 2009.09.01:

- Support for AIX VIO Server 2.1 on AIX 6.1

- Support for Logical Partition (LPAR) on AIX 5.3 and 6.1
- Support for SUSE 11 on x86, Opteron and EM64T, Itanium, zLinux (s390x), and PPC e-Server
- Support for RHEL 5.2 and 5.3 on x86, Opteron and EM64T, Itanium, zLinux (s390x), and PPC e-Server
- Support for Oracle Enterprise Linux 5.2, 5.3 on x86, Opteron and EM64T
- Support for Hyper-V Server 2008
- Support for SUSE OES 2 SP1 on x86 and Opteron and EM64T
- Support for ESX server 4.0 on x86 and Opteron and EM64T
- One new IIS Configuration (Windows) module with seven checks and two templates.
- One new check in the Active Directory (Windows) module
- One new check in the Agent Information (Windows and UNIX) module
- One new check in the Login Parameters (UNIX) module
- One new check in the Network Integrity (UNIX) module
- One new check in the OS Patches (AIX VIO Server) module
- One new check in the Password Strength (UNIX) module
- One new message in the Symantec Product Information (Windows) module
- One new message in the Password Strength (UNIX) module
- One new template in the Login Parameters (UNIX) module
- One new template in the Object Integrity (UNIX) module
- One new template in the OS Patches (AIX) module
- One new template in the Password Strength (UNIX) module
- Enhancements in the Login Parameters, File Find, System Auditing, Network Integrity, and User Files modules.

On the LiveUpdate Wizard, the SU version is now visible in the following format: SU<YYYY>.<MM>.<Release_Version>. Where, YYYY is the year of release, MM is the month of release, and Release_Version is the release version of the SU. For example, SU 38 displays as SU 2009.09.01 on the LiveUpdate Wizard.

About the new operating systems support

SU 2009.09.01 provides support for the following operating systems:

- Support for AIX VIO Server 2.1 on AIX 6.1
  The ESM 6.5.3 SP2 and later AIX-PPC64 agents are now certified on AIX VIO Server 2.1. To use this agent, install the existing AIX-PPC64 agent and apply SU 2009.09.01 to it.
  See "About the VIO Server" on page 10.
- Support for Logical Partitions (LPARs) on AIX 5.3 and 6.1
  The ESM 6.5.3 SP2 and later AIX-PPC64 agents are now certified on AIX 6.1 Logical Partition (LPAR). You can use a corresponding agent on the LPAR operating system. For example, if SUSE 10 partition is installed on an ESM agent computer then use LNX-PPC64 agent.
- Support for ESX server 4.0
  The ESM 6.5.3 SP2 and later Linux -x86 agent is certified on ESX server 4.0.
- Support for Hyper-V Server 2008
  The ESM 6.5.3 SP2 and later agents are now certified on Windows 2008 Hyper-V Server. To use this agent, install the existing Windows 2008 agents and apply SU 2009.09.01 to it.
- Support for Oracle Enterprise Linux 5.2 and 5.3 on x86, Opteron and EM64T
  The ESM 6.5.3 SP2 and later agents are now certified on Oracle Enterprise Linux on 5.2 and 5.3. To use this agent, install the existing x86 and Opteron Linux agents and apply SU 2009.09.01 to it.
- Support for SUSE OES 2 SP1 on x86 and Opteron and EM64T
  The ESM 6.5.3 SP2 and later agents are now certified on OES 2 SP1 on x86 and Opteron and EM64T. To use this agent, install the existing x86 and Opteron Linux agents and apply SU 2009.09.01 to it.
- Support for RHEL 5.2 and 5.3 on x86, Opteron and EM64T, Itanium, zLinux (s390x), and PPC e-Server
  The ESM 6.5.3 SP2 and later agents are now certified on Red Hat Enterprise Linux Server 5.2 and 5.3 on x86, Opteron and EM64T, Itanium, zLinux (s390x), and PPC e-Server. To use this agent, install the existing agent and apply SU 2009.09.01 to it.
- Support for SUSE 11 on x86, Opteron and EM64T, Itanium, zLinux (s390x), and PPC e-Server
  The ESM 6.5.3 SP2 and later agents are now certified on SUSE 11 x86, Opteron and EM64T, Itanium, zLinux (s390x), and PPC e-Server. To use this agent, install the existing agent and apply SU 2009.09.01 to it.

For more information on the agents, refer to ESM Agent Downloads section on the following Symantec Security Response Web site:

http://www.symantec.com/avcenter/security/Content/Product/Product_ESM.html

About the VIO Server

This section explains the steps that you can follow to install the ESM installer (tpk) on the VIO Server and its CPU and Memory usage.

How to install the ESM installer on the VIO Server

To install the ESM installer on the VIO Server

1. Logon as root.
2. Execute the `oem_setup_env` command.

   The `oem_setup_env` command places the padmin user in a non-restricted UNIX root shell.
3. Run the **esm_aix_ppc64.tpk** installer.

About CPU and Memory usage

The ESM agent process remains idle when no policy run takes place. You may observe spikes in the CPU and memory usage when you execute one or multiple checks, as these checks may contend for the CPU time slice. This performance of the ESM agent is in-line with other operating systems like Solaris, Linux, and HP-UX.

New Module

SU 2009.09.01 adds the following new module:

- IIS Configuration (Windows)

IIS Configuration (Windows)

The checks in the IIS Configuration module on Windows verify the various settings that are associated with the IIS server on the ESM agent computer. Out of the seven new checks, two are template-based checks.

Following are the template-based checks:

- ASP.Net Configuration
- Metabase settings

The **ASP.Net Configuration** check uses the IIS ASP.NET template to report on the ASP.Net configuration settings that you specify in the template against the settings that are found on the IIS server. See "About the Templates in the IIS Configuration (Windows)" on page 14.

The **Metabase settings** check uses the IIS Metabase template that reports on the metabase settings that you specify in the template against the settings that are found on the IIS server. See "About the Templates in the IIS Configuration (Windows)" on page 14.

About the Checks in the IIS Configuration (Windows)

SU 2009.09.01 adds seven checks in the IIS Configuration module on Windows:

- ASP.Net Configuration
- Log directory
- Metabase settings
- Virtual directory
- WAMUser
- Web site
- Web sites and Virtual directories

Web site

This check reports the name, path, port, and status of the Web sites that are present on the IIS server of the ESM agent computer.

Table 1-1 lists the message that this check reports.

Table 1-1 Message for the Web site check

Message ID	Message Title	Message Severity
ESM_IISMETAWEBSITE	Web site	Green-0

Virtual directory

This check reports the virtual directory name, complete hierarchical path, directory type, and directory path of the virtual directories that are present in the Web sites, FTP sites, SMTP server, and NNTP server of the ESM agent computer.

Table 1-2 lists the message that this check reports.

Table 1-2 Message for the Virtual directory check

Message ID	Message Title	Message Severity
ESM_IISMETAVIRTUALDIR	Virtual directory	Green-0

Log directory

This check reports the directory that is set for logging and the name of the Web sites, FTP sites, SMTP server and NNTP server that are present on the ESM agent computer.

Table 1-3 lists the message that this check reports.

Table 1-3 Message for the Log directory check

Message ID	Message Title	Message Severity
ESM_IISMETALOGDIR	Log directory	Green-0
ESM_IISMETALOGDISABLED	Logging disabled	Yellow-1

WAMUser

This check reports the configuration user name that is configured with the Application pool.

Table 1-4 lists the message that this check reports.

Table 1-4 Message for the WAMUser check

Message ID	Message Title	Message Severity
ESM_IISMETAWAMUSER	WAMUser	Green-0

Metabase settings

This check validates the current IIS metabase settings that are found on the Web site, virtual directory, FTP site, and other components with the settings that you specify in the Metabase setting template. The module reports the following:

- Mandatory IIS Metabase keys and values that do not exist on the ESM agent computers.
- Forbidden keys and values that exist on the ESM agent computers.

Use the IIS Metabase template to define the keys and the values for the check to report on.

Table 1-5 lists the message that this check reports.

Table 1-5 Message for the Metabase settings check

Message ID	Message Title	Message Severity
ESM_IISMETA_NOEXISTKEY	Mandatory IIS metabase key does not exist	Red-4

Table 1-5 Message for the Metabase settings check *(continued)*

Message ID	Message Title	Message Severity
ESM_IISMETA_ NOEXISTVALUE	Mandatory IIS metabase value does not exist	Red-4
ESM_IISMETA_FORBIDKEY	Forbidden IIS metabase key exists	Red-4
ESM_IISMETA_FORBIDVALUE	Forbidden IIS metabase value exists	Red-4

The check may report incorrect results for the hidden Metabase properties where the MetaFlagsEx attribute is set as Hidden.

Note: This check does not support IIS 7.0. However, this check reports on the metabase properties that can be configured using the IIS Management Compatibility feature when this feature is enabled during installation.

ASP.NET Configuration

This check validates the current IIS ASP.NET configuration settings that are found on the ESM agent computer with the settings that you specify in the IIS ASP.Net template. This check works with the **Web sites and Virtual directories** check to report on the virtual directories or Web sites that you specify in the **Web sites and Virtual directories** name list.

Table 1-6 lists the message that this check reports.

Table 1-6 Message for the ASP.NET Configuration check

Message ID	Message Title	Message Severity
ESM_IISASP_ UNEXPECTED_VALUE	IIS ASP.NET Configuration setting's unexpected value exists	Red-4
ESM_IISASP_ SETTING_NOT_FOUND	IIS ASP.NET Configuration setting not found	Red-4
ESM_IISASP_ INVALID_SETTING	IIS ASP.Net Configuration setting is invalid	Red-4
ESM_IIS_NOT_FOUND	.Net Framework is unavailable	Red-4

The check reports on the following default settings if it finds an IIS 5.0 Isolation mode enabled:

- COM Authentication Level
- COM Impersonation Level
- Client Connected Check Timeout
- Cpu Mask
- Idle Timeout
- Worker Process Shutdown Timeout
- Worker Process Password
- Worker Process Username
- Process Model Enabled
- Web Garden
- Mem Limit
- Request Limit
- Request Queue Limit
- Restart Process Queue Limit

The check ignores these settings if the **Worker Process Isolation Mode** is found enabled on IIS 6.0. In this case, you can use the **Metabase settings** check to report on the settings that are configured on the Application pool.

Web sites and Virtual directories

This check works with the **ASP.NET configuration** check. Use this name list to include or exclude the Web sites and Virtual directories that the **ASP.NET configuration** check should report on. For example, Website1/VirtualDir1.

About the Templates in the IIS Configuration (Windows)

SU 2009.09.01 adds the following templates in the IIS Configuration module on Windows:

- IIS Metabase template in the IIS Configuration module on Windows
- IIS ASP.Net template in the IIS Configuration module on Windows

IIS Metabase (Windows IIS Configuration)

The **Metabase settings** check uses the IIS Metabase template to report on the metabase settings that you specify in the template against the settings that are found on the IIS server.

The IIS Metabase template has a default .iis extension.

Creating the IIS Metabase template

You must create and enable a new IIS Metabase template before you run the **Metabase settings** check in the IIS Configuration module.

To create a new IIS Metabase template

1. In the tree view, right-click **Templates**, then click **New**.
2. In the **Create New Template** dialog box, select **IIS Metabase-all**.
3. In the **Template file name (no extension)** text box, type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .iis extension to the template file name.
4. Click **OK**.

About using the IIS Metabase template

The IIS Metabase template contains the following fields:

IIS Object Name

Specify the name of the object that is present in the IIS server.

The following objects are supported:

- Web sites
- FTP sites
- Virtual directories
- SMTP server
- NNTP server
- Application pool

See "About using the IIS Object Name column" on page 18.

IIS Object Type

Specify the object type.

Following are the supported IIS Object types:

- Web sites
- FTP sites
- Virtual directories
- SMTP server
- NNTP server
- Application pool

For Example:

- To report on the virtual directories that can be present on the Web sites and FTP sites, enter **Web site\VirtualDirectory** in the **IIS Objects Name** column and select **IIsWebVirtualDir** option from the **IIS Object Type** drop-down list.
- To report on the virtual directories that can be present on the NNTP sites, enter an NNTP virtual directory name in the **IIS Objects Name** column and select **IIsNntpVirtualDir** option from the **IIS Object Type** drop-down list.
- To report on the virtual directories that can be present on the FTP sites, enter an FTP virtual directory name in the **IIS Objects Name** column and select **IIsFtpVirtualDir** option from the **IIS Object Type** drop-down list.
- To report on the virtual directories that can be present on the SMTP sites, enter an SMTP virtual directory name in the **IIS Objects Name** column and select **IIsSmtpVirtualDir** option from the **IIS Object Type** drop-down list.
- To report on an FTP site, enter an FTP site name in the **IIS Objects Name** column and select **IIsFtpServer** option from the **IIS Object Type** drop-down list.
- To report on a Web site, enter a Web site name in the **IIS Objects Name** column and select **IIsWebServer** option from the **IIS Object Type** drop-down list.
- To report on an NNTP virtual server, enter an NNTP virtual server name in the **IIS Objects Name** column and select **IIsNntpServer** option from the **IIS Object Type** drop-down list.
- To report on an SMTP virtual server, enter an SMTP virtual server name in the **IIS Objects Name** column and select **IIsSmtpServer** option from the **IIS Object Type** drop-down list.
- To report on an Application pool option, enter an Application pool name and select **IIsApplicationPool** option from the **IIS Object Type** drop-down list.

See "About using the IIS Object Name column" on page 18.

Required

Specify one of the following:

- Optional
  The check ignores the presence of IIS Object and continues to report on the Data Existence.
- Mandatory
  The check reports if the key that you specify in the **IIS Object Name** field does not exist on the ESM agent computer.
- Forbidden
  The check reports if the key that you specify in the **IIS Object Name** exists on the ESM agent computer.

Data Existence

Specify the Metabase property entries for the **Metabase settings** check.

The **Template Sublist Editor** contains the following fields:

- Attribute Name
  Specify the name of the Metabase property.
- Attribute Value
  Specify the value of the Metabase property.
  You can specify the following two types of value:
  - You can specify a string or an integer (numeric value) that is present in the *Metabase.xml* file, if you do not select the **Bitmask Data** check box.
  - You can enter a flag value, if you select the **Bitmask Data** check box. You can use a Pipe (|) to separate the multiple flags. For example, AccessRead | AccessWrite.

  Note: You can use POSIX regular expressions to report on multiple entries. The newline character is not supported.
- Required
  You can specify the following two types of value:
  - Mandatory
    The check reports if the Metabase property is not configured or if the property value does not match on the ESM agent computer.
  - Forbidden
    The check reports if the Metabase property is configured or if the property value matches on the ESM agent computer.
- Bitmask Data
  Select this check box if you enter the Metabase flag properties in the **Attribute Name** field.
  For example: AccessFlag = "AccessRead | AccessWrite".
- Comment
  Specify an additional comment.

Comment	Specify an additional comment.

See "New Checks" on page 20.

About using the IIS Object Name column

You can specifically use this column to report on the virtual directories, if the object type that you select is a virtual directory.

To report on the virtual directories that are present on the Web sites or FTP sites, in the **IIS Object Name** column, do one of the following:

- To report on the virtual directories that match the name 'SampleVirtualdirectory', enter **SampleVirtualdirectory** in the **IIS Object Name** column. The check reports on the matching virtual directories that are present on any Web sites or FTP sites. You can use **SampleVirtualdirectory$** to find an exact match of the SampleVirtualdirectory.
- To report on multiple hierarchy virtual directories 'SampleVirtualdirectory1/SampleVirtualdirectory2' on the Web sites and FTP sites, enter **SampleVirtualdirectory1/SampleVirtualdirectory2** in the **IIS Object Name** column. Use a forward slash (/) to separate multiple virtual directories.
- To report on the virtual directories that match the name 'SampleVirtualdirectory1' for the Site 'Sample Web site1', enter **Sample Web site1\SampleVirtualdirectory1** in the **IIS Object Name** column. Use a backward slash (\) to separate the site name and the virtual directory name.
- To report on multiple hierarchy virtual directories 'SampleVirtualdirectory1/SampleVirtualdirectory2' for the site 'Sample Web site2', enter **Sample Web site2\SampleVirtualdirectory1/SampleVirtualdirectory2** in the **IIS Object Name** column.

Note: This column supports POSIX regular expressions. For example, if you want the check to report on SampleVirtualdirectory1 from the Sample Web site 1 and 2 then in the **IIS Object Name** column enter **Sample Web site*\SampleVirtualdirectory1**.

IIS ASP.Net (Windows IIS Configuration)

The **ASP.Net Configuration** check uses the IIS ASP.NET template to report on the ASP.Net configuration settings that you specify in the template against the settings that are found on the IIS server. The default template is available for each supported operating system.

The IIS ASP.Net template has a default .aps extension.

Note: You cannot edit the default template however; you can duplicate an existing template. The **Configuration Setting** field is pre-populated with default values. As the check only reports on the default values, you must not modify the **Configuration Setting** field.

Creating the IIS ASP.Net template

You cannot edit the default template; however, you can duplicate an existing template. The **Configuration Setting** field is pre-populated with default values. As the check only reports on the default values, you must not modify the **Configuration Setting** field. You can however; update the **Expected Value Regular Expression** field or modify the **Enabled** check box setting.

To duplicate an IIS ASP.Net template

1. In the tree view, expand the **Templates** list, and go to IIS ASP.Net-all (aspdotnet.aps).
2. Right-click **IIS ASP.Net-all (aspdotnet.aps)** and click **Duplicate**.
3. In the **Copy Template** dialog box, type a new template file name of no more than eight characters, without a file extension, without a file extension. Symantec ESM adds the .aps extension to the file name.
4. Click **OK**.

About using the IIS ASP.Net template

The IIS ASP.NET template contains the following fields:

Enabled	Select this check box if you want the check to report on the settings.
Configuration Setting	This field displays the ASP.NET settings that are supported by the **ASP.NET Configuration** check. **Note:** The check reports an error message if you change the default values or add new values in the **Configuration Settings** field. The check only reports on the default settings.
Expected Value Regular Expression	Enter a value of an ASP.NET Configuration or a POSIX regular expression.
Comments	Enter an additional comment.

See "New Checks" on page 20.

New Checks

SU 2009.09.01 adds new checks in the following modules:

- Active Directory (Windows)
- Agent Information (Windows and UNIX)
- Login Parameters (UNIX)
- Network Integrity (UNIX)
- OS Patches (AIX VIO Server)
- Password Strength (UNIX)

Active Directory (Windows)

SU 2009.09.01 adds one new check in the Active Directory module on Windows:

- Domain Controller Information

Domain Controller Information

This check is only applicable on a domain controller. The check verifies whether the ESM agent computer is a global catalog. On a Windows 2008 server, this check also reports whether a domain controller is read-only or read-write.

Table 1-7 lists the message that this check reports.

Table 1-7 Message for the Domain Controller Information check

Message ID	Message Title	Message Severity
ESM_DC_INFO	Domain Controller information	Green-0
ESM_DC_INFO_ERROR	Error while collecting Domain Controller information	Red-4

Agent Information (Windows and UNIX)

SU 2009.09.01 adds one new check in the Agent Information module on Windows and UNIX:

- LiveUpdate status

LiveUpdate status

This check reports whether LiveUpdate is enabled or disabled on the ESM agent computer.

Table 1-8 lists the message that this check reports.

Table 1-8 Message for the LiveUpdate status check

Message ID	Message Title	Message Severity
ESM_LIVEUPDATE_ENABLED	ESM LiveUpdate is enabled	Green-0
ESM_LIVEUPDATE_DISABLED	ESM LiveUpdate is disabled	Green-0

Login Parameters (UNIX)

SU 2009.09.01 adds one new check in the Login Parameters module on UNIX:

- Required PAM Configuration

Required PAM Configuration

Use this check to specify the PAM configuration settings in the template. You should add those PAM modules in the template that are used for local authentication. If this check cannot find these settings on the ESM agent computer, then ESM does not execute the checks that you select in the template.

Note: This check does not report if the PAM configuration in the `/etc/pam.conf` file invokes another module.

For Example, login auth required pam_auth_lock.so call pam_unix_auth.so.

Note: This check does not report if the PAM configuration specifies a different service in the `/etc/pam.conf` file. For Example, password required pam_stack.so service=system-auth.

See "New Templates" on page 24.

Network Integrity (UNIX)

SU 2009.09.01 adds one new check in the Network Integrity module on UNIX:

- Established TCP connection

Established TCP connection

This check reports the TCP ports with the established status and the process name that opens the port if the `/usr/sbin/lsof` or `/usr/bin/lsof` programs exist on the ESM agent computer.

Table 1-9 lists the messages that this check reports.

Table 1-9 Message for the Established TCP connection

Message ID	Message Title	Message Severity
STKU_ESTABLISHED_PORT	Connected ports	red-4

OS Patches (AIX VIO Server)

SU 2009.09.01 adds one new check in the OS Patches module on AIX VIO Server:

- VIOS level

VIOS level

This check reports if the latest VIOS level that you specify in the template is not found on the ESM agent computer.

Table 1-10 lists the message that this check reports.

Table 1-10 Messages for the VIOS level check

Message ID	Message Title	Message Severity
ESM_NO_ TEMPLATE_SPECIFIED	No applicable template files specified	Red-4
VIOS_REQUIRED_FIXPACK	Required VIOS level for your computer	Red-4

See "New Templates" on page 24.

Password Strength (UNIX)

SU 2009.09.01 adds one new check in the Password Strength module on UNIX:

- Required PAM Configuration

Required PAM Configuration

Use this check to specify the PAM configuration settings in the template. You should add those PAM modules in the template that are used for local authentication. If this check cannot find these settings on the ESM agent computer, then ESM does not execute the checks that you select in the template.

Note: This check does not report if the PAM configuration specifies a different service in the `/etc/pam.conf` file. For Example, password required pam_stack.so service=system-auth.

Note: This check does not report if the PAM configuration in the `/etc/pam.conf` file invokes another module.

For Example, login auth required pam_auth_lock.so call pam_unix_auth.so.

See "New Templates" on page 24.

New Messages

SU 2009.09.01 adds new messages to the following checks:

- Symantec Endpoint Protection (SEP) group (Windows Symantec Product Information)
- Password age (UNIX Password Strength)

Symantec Endpoint Protection (SEP) group (Windows Symantec Product Information)

A new message 'This Setting is not found' has been added to the following checks in the Symantec Product Information (Windows) module under the Symantec Endpoint Protection (SEP) group:

- LiveUpdate frequency
- Scan frequency
- Maximum Virus Definition File age
- File System Auto-Protected
- Internet Email Auto-Protected
- Outlook Auto-Protected

This message is reported when the check is unable to find the SEP's registry key on the ESM agent computer.

Password age (UNIX Password Strength)

A new message has been added to the **Password age** check in the Password Strength module. This message is reported if you have not changed your password within the specified number of days.

Table 1-11 lists the new message

Table 1-11 New message for the Password age check

Message ID	Message Title	Message Severity
STKU_PASS_NEVER_CHANGED	Password never changed	Yellow-3

New Templates

SU 2009.09.01 adds the following new templates:

- Name To Major template in the Object Integrity module on UNIX
- PAM Conf for Login Parameters template in the Login Parameters module on UNIX
- PAM Conf for Password Strength in the Password Strength module on UNIX
- VIOS level template in the OS Patches module on AIX

Name To Major (UNIX Object Integrity)

The **Disk and memory access** check uses the Name To Major template to report on the values that you specify in the template.

The Name To Major template has a default .ntm extension.

Creating the Name To Major template

You must create and enable a new Name To Major template before you run the **Disk and memory access** check in the Object Integrity module.

To create a new Name To Major template

1. In the tree view, right-click **Templates**, then click **New**.
2. In the **Create New Template** dialog box, select **Name To Major-all**.

3 In the **Template file name (no extension)** text box, type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .ntm extension to the template file name.

4 Click **OK**.

About using the Name To Major template

The Name To Major template contains the following fields:

OS/Rev	Specify the operating systems and their revisions. ■ Exclude Select this check box to exclude the specified operating system and revision from checks in the template or uncheck it to include the operating system and revision. ■ OS Select the value that describes the operating system or systems that you want to exclude or include for enabled checks. ■ Release/Revision Specify a revision ID for the operating system that you selected.
Device Name	Specify the details of device for the check to report on. The**Device Name Template Sublist Editor** contains the following fields: ■ Name To Major Number Enter a device name or Major number. ■ Device type Specify the type of device. On Linux for example, If the USB device has 180 as a major number, then enter **180** in the **Name or Major Number** field and enter memory in the **Device Type** field.
Comment	Specify an additional comment.

PAM Conf for Login Parameters (UNIX Login Parameters)

The **Required PAM Configuration** check uses the PAM Conf for Login Parameters template to report on the PAM configuration settings that you specify for the checks that you select in the template.

The PAM Conf for Login Parameters template has a default .lpl extension.

Creating the PAM Conf Login Parameters template

You must create and enable a new PAM Conf Login Parameters template before you run the **Required PAM Configuration** check in the Login Parameters module.

To create a new PAM Conf Login Parameters template

1. In the tree view, right-click **Templates**, then click **New**.
2. In the **Create New Template** dialog box, select **PAM Conf Login Parameters-all**.
3. In the **Template file name (no extension)** text box, type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .lpl extension to the template file name.
4. Click **OK**.

About using the PAM Conf Login Parameters template

The PAM Conf Login Parameters template contains the following fields:

OS/Rev	Specify the operating systems and their revisions. ■ Exclude Select this check box to exclude the specified operating system and revision from checks in the template or uncheck it to include the operating system and revision. ■ OS Select the value that describes the operating system or systems that you want to exclude or include for enabled checks. ■ Release/Revision Specify a revision ID for the operating system that you selected.
Check Name	Select the check name that you want to enable. If the Pam Configuration that you specify in the **Pam entry Template Sublist Editor** matches with the PAM Configuration of the ESM Agent computer, then ESM executes the check that you select. If the PAM configuration is not found on the ESM Agent Computer, then ESM does not execute the check that you select.

Pam entry

Specify the PAM configuration value for the check to report on for local authentication.

The **Pam entry Template Sublist Editor** contains the following fields:

- Service name
  Enter the name of the service.
- Module type
  Specify the type of the module.
- Library
  Specify the library setting.

On Linux, if the `/etc/pam.d/su` file has the following entry:

auth sufficient pam_rootok.so

You can enter the following values in the **Pam entry Template Sublist Editor**:

- Service name
  su
- Module type
  auth
- Library
  pam_rootok.so

On UNIX, if the `/etc/pam.conf` file has the following entry:

ftp session required pam_aix

You can enter the following values in the **Pam entry Template Sublist Editor**:

- Service name
  ftp
- Module type
  session
- Library
  pam_aix

If you enter **All** in the **Service name** field, then the check matches all the files or all the services that are found in the `/etc/pam.d` folder and the `/etc/pam.conf` file. If the check finds a match of the **Module type** and the **Library** on the ESM agent computer, then the module executes the check that you have selected in the template.

See "New Checks" on page 20.

PAM Conf for Password Strength (UNIX Password Strength)

The **Required PAM Configuration** check uses the PAM Conf for Password Strength template to report on the PAM configuration settings that you specify for the checks that you select in the template.

The PAM Conf for Password Strength template has a default .ppl extension.

Creating the PAM Conf for Password Strength template

You must create and enable a new PAM Conf for Password Strength template before you run the **Required PAM Configuration** check in the Password Strength module.

To create a new PAM Conf for Password Strength template

1. In the tree view, right-click **Templates**, then click **New**.
2. In the **Create New Template** dialog box, select **PAM Conf for Password Strength-all**.
3. In the **Template file name (no extension)** text box, type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .ppl extension to the template file name.
4. Click **OK**.

About using the PAM Conf for Password Strength template

The PAM Conf for Password Strength template contains the following fields:

OS/Rev

Specify the operating systems and their revisions.

- Exclude
  Select this check box to exclude the specified operating system and revision from checks in the template or uncheck it to include the operating system and revision.
- OS
  Select the value that describes the operating system or systems that you want to exclude or include for enabled checks.
- Release/Revision
  Specify a revision ID for the operating system that you selected.

Check Name	Select the check name that you want to enable. If the Pam Configuration that you specify in the **Pam entry Template Sublist Editor** matches with the PAM Configuration of the ESM Agent computer, then ESM executes the check that you select. If the PAM configuration is not found on the ESM Agent Computer, then ESM does not execute the check that you select.

Pam entry

Specify the PAM configuration value for the check to report on for local authentication.

The **Pam entry Template Sublist Editor** contains the following fields:

- Service name
  Enter the name of the service.
- Module type
  Specify the type of the module.
- Library
  Specify the library setting.

On Linux, if the `/etc/pam.d/su` file has the following entry:

auth sufficient pam_rootok.so

You can enter the following values in the **Pam entry Template Sublist Editor**:

- Service name
  su
- Module type
  auth
- Library
  pam_rootok.so

On UNIX, if the `/etc/pam.conf` file has the following entry:

ftp session required pam_aix

You can enter the following values in the **Pam entry Template Sublist Editor**:

- Service name
  ftp
- Module type
  session
- Library
  pam_aix

If you enter **All** in the **Service name** field, then the check matches all the files or all the services that are found in the `/etc/pam.d` folder and the `/etc/pam.conf` file. If the check finds a match of the **Module type** and the **Library** on the ESM agent computer, then the module executes the check that you have selected in the template.

See "New Checks" on page 20.

VIOS level (AIX OS Patches)

The **VIOS level** check uses the VIOS level template to report on the VIOS level that you specify in the template against the VIOS level that are present on the ESM agent computer.

The VIOS level template has a default .pvio extension.

Creating the VIOS level template

You must create and enable a new VIOS level template before you run the **VIOS level** check in the OS Patches module.

To create a new VIOS level template

1. In the tree view, right-click **Templates**, then click **New**.
2. In the **Create New Template** dialog box, select **VIOS level - AIX**.
3. In the **Template file name (no extension)** text box, type a new template file name of no more than eight characters, without a file extension. Symantec ESM adds the .pvio extension to the template file name.
4. Click **OK**.

About using the VIOS level template

The VIOS level template contains the following fields:

VIOS Version	Enter the current version on which you want the check to report on. For Example, 2.1.
Required VIOS level	Enter the VOIS level. The check verifies whether the level that you specify in this column is present on the ESM agent computer. If you mention multiple levels that have the same VIOS version, then the check reports on the higher version. The required VIOS level is determined through the latest available Fix pack or Service pack.
Release date	Enter the release date of the Fix pack or the Service pack.
Comments	Specify an additional comment. You can also specify the name of the Fix pack or the Service pack.

See “New Checks” on page 20.

Modified Templates

The following template has been modified:

- Shells (UNIX Account Integrity)

Shells (UNIX Account Integrity)

A new OS/Rev sublist has been added to the Shells template for the **User Shell Compliance** check in the Account Integrity module. The check reports on the platforms that you include or exclude in the OS/Rev sublist.

You can specify the following values in the required columns:

Exclude	Check this check box to exclude the platform for the **User Shell Compliance** check.
OS	Specify the operating system that you want the check to report on.
Release/Revision	Specify the version of the operating system that you want to include.

System requirements

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

Note: Per End of Life product support policy, ESM content updates on ESM 6.0 is not supported from SU 2008.09.01.

Table 1-12 includes the supported operating systems for SU 2009.09.01.

Table 1-12 Supported operating systems for SU 2009.09.01

Agent operating system	Platform	Supported versions on 6.5 and later
AIX	PPC64	VIO client version 1.5 on AIX 6.1
AIX	PPC64	VIO Server 2.1 on AIX 6.1
AIX	RS 6000	5.2 (32-bit and 64-bit) 5.3 (32-bit only)

Table 1-12 Supported operating systems for SU 2009.09.01 *(continued)*

Agent operating system	Platform	Supported versions on 6.5 and later
AIX	PPC64	5.3 (64-bit only) 6.1
AIX	PPC64	WPAR on 6.1
AIX	PPC64	LPAR on AIX 5.3 and 6.1
ESX Server	x86, Opteron and EM64T	3.0.2, 3.5, 4.0
HP-UX	PA-RISC	11.11, 11.23, 11.31
HP-UX	Itanium®	11.23, 11.31
Hyper-V Server 2008	Opteron and EM64T	SP1
Oracle Enterprise Linux	x86 and Opteron	5.2, 5.3
SUSE OES	x86 and Opteron and EM64T	2SP1, SP2
Red Hat Enterprise Linux	IBM zSeries (s390x)	5.0, 5.2, 5.3
Red Hat Enterprise Linux ES	x86, Opteron and EM64T	3.0, 4.0
Red Hat Enterprise Linux Server	x86, Opteron and EM64T, and Itanium®	5.0, 5.1, 5.2, 5.3
Red Hat Enterprise Linux Server	IBM PPC e-Server	5.0, 5.2, 5.3
Red Hat Enterprise Linux WS and AS	x86, Opteron and EM64T	3.0, 4.0
Red Hat Enterprise Linux AS	Itanium®	3.0, 4.0
Sun Solaris	SPARC	2.8, 2.9, 2.10 2.10 Local zone
Sun Solaris	x86, Opteron and EM64T	2.10
SUSE Linux	IBM zSeries (s390x)	9 SP4 10 SP1
SUSE Linux Standard Server	x86	9, 9 SP4

Table 1-12 Supported operating systems for SU 2009.09.01 *(continued)*

Agent operating system	Platform	Supported versions on 6.5 and later
SUSE Linux Enterprise Server	x86	9, 9 SP4 10, 10 SP2, 11
SUSE Linux Enterprise Server	Itanium®	9, 9 SP4 10, 10 SP2, 11
SUSE Linux Enterprise Server	Opteron and EM64T	9, 9 SP4 10, 10 SP2, 11
SUSE Linux Enterprise Server	IBM PPC e-Server	9, 9 SP4 10, 10 SP2, 11
SUSE Linux Enterprise Server	IBM zSeries	9, 9 SP4 10, 10 SP1, 11
Windows 2000 Professional and Server	x86	All
Windows Server 2003	x86	SP0, SP1, SP2
Windows Server 2003	Itanium®	SP0, SP1, SP2
Windows Server 2003 Enterprise	Opteron and EM64T	SP0, SP1, SP2
Windows Vista	x86	SP0, SP1 Enterprise and Business editions SP1
Windows Vista	Opteron and EM64T	SP0, SP1 Enterprise and Business editions SP1
Windows XP Professional	x86	SP2 SP3
Windows Server 2008	x86	SP1 and SP2
Windows Server 2008	Opteron and EM64T	SP1 and SP2
Windows Server 2008	Itanium®	SP1 and SP2

Table 1-12 Supported operating systems for SU 2009.09.01 *(continued)*

Agent operating system	Platform	Supported versions on 6.5 and later
Windows Server 2008 Core Installation	x86	SP1 and SP2
Windows Server 2008 Core Installation	Opteron and EM64T	SP1 and SP2

Table 1-13 lists the disk space usage for an ESM 9.0 SP1 agent with SU2009.09.01 applied. The amount of disk space that is required by each agent depends on its operating system.

Table 1-13 Agent disk space requirements for SU 2009.09.01

Agent operating system	Disk space required (in MB)
AIX /RS 6000	270
AIX (PPC64)	305
HP-UX (HPPA)	140
HP-UX (Itanium®)	210
Red Hat Linux, SuSE Linux (x86)	105
Red Hat Linux, SuSE Linux (PPC64)	85
Red Hat Linux, SuSE Linux (AMD64, EM64T)	105
Red Hat Linux, SuSE Linux (Itanium®)	140
Red Hat Linux, SuSE Linux (s390x)	100
Sun Solaris (SPARC)	105
Sun Solaris (x86, Opteron and EM64T)	130
Windows 2000 (x86)	85
Windows Server 2003 (x86)	85
Windows Server 2003 (Itanium®)	170
Windows Server 2003 (Opteron and EM64T)	100
Windows XP (x86)	75

Table 1-13 Agent disk space requirements for SU 2009.09.01 *(continued)*

Agent operating system	Disk space required (in MB)
Windows Vista (x86)	70
Windows Vista (Opteron and EM64T)	100
Windows Server 2008 (x86)	70
Windows Server 2008 (Itanium®)	150
Windows Server 2008 (Opteron and EM64T)	95

Enhancements

The following modules and checks have been enhanced in SU 2009.09.01:

File Find (UNIX)	The check **Global Zone Only** has been modified to exclude the file systems that have been mounted from a global zone to the local zones in the Read-Write mode.

File Find (UNIX)

The check **World writable files** now reports on the files that are present in the directories that are not world writable.

This check is also modified to support the **Skip files in not WW directory** text box.

In the **Skip files in not WW directory** text box, do one of the following:

- Set the value to 0.
  The check does not report on the files that are present in the directories that are not world writable.
- Set the value to 1.
  The check reports on the files that are present in the directories that are not world writable.

The check **Group writable files** now reports on the files that are present in the directories that are not group writable.

This check is also modified to support the **Skip files in not GW directory** text box.

In the **Skip files in not GW directory** text box, do one of the following:

- Set the value to 0.
  The check does not report on the files that are present in the directories that are not group writable.
- Set the value to 1.
  The check reports on the files that are present in the directories that are not group writable.

Login Parameters (UNIX)

The check **Warning Banners** has been modified to report on the banners that have been placed at different locations by the TCP Wrapper software.

The check **Warning banners** has also been enhanced to look for appropriate warning banners in the /etc/motd, /etc/issue , /etc/default/telnetd, and /etc/default/ftpd (/etc/fptd/ftpaccess on Solaris 9 and 10 and HP-UX 11.11, 11.23, and 11.31) files.

Network Integrity (UNIX)	The check **NFS exported directory anonymous access** is now supported on Linux ESM agent computers.
Network Integrity (UNIX)	The module has been enhanced to provide the vsftpd support on the following platforms: ■ Red Hat Linux ■ SUSE Linux ■ HP-UX ■ Solaris ■ AIX The module has been enhanced to report on following user files: ■ User files `/etc/vsftpd/ftpusers` that PAM module (pam_listfiles.so) uses in the vsftpd PAM service file `/etc/pam.d/vsftpd`. ■ User files that vsftpd uses. For example, `/etc/vsftpd/user_list`.
OS Patches (Linux)	The **Revision** column in the Patch.plx template has been enhanced to report on the Oracle Enterprise Linux (OEL). In the **Revision** column, you should enter the revision number followed by OEL. For example, 4.0OEL. You can get the revision number by executing the `/bin/rpm -q --qf %{VERSION} enterprise-release` command.
OS Patches (AIX)	The module has been enhanced to support the Service Pack information level on the AIX ESM agent computers.
System Auditing (UNIX)	The check **Auditing enabled** is now supported on Linux ESM agent computers. **Note:** You must have auditctl binary present on the ESM agent computer.

User Files (UNIX)

The check **Umask (parsing startup scripts)** is now enhanced to report on all the startup scripts that are included in the name list, if the Umask parameters that are found are less than the value that you specify in the **Minimum umask value** text box of the **Umask** check.

The check **Umask (parsing startup scripts)** is also modified to support the **Listing all finding** text box where the check reports all the parameters that it has found.

- If the value is 0, the check reports only the minimum value that is found then the value that you specify in the **Minimum umask value** text box.
- If the value is 1, then the check reports on all the startup scripts that are listed in the name list, if the Umask parameters that are found are less than the value that you specify in the **Minimum umask value** text box.

Resolved issues

The following issues are resolved in SU 2009.09.01:

Account Integrity (Windows)

The check **Accounts must be disabled** has been modified to report the accounts that are included in the **Users and Groups** name lists of the check in the following formats:

On a Domain Controller

- Domain\User
- Domain\Group
- %User%
- %Group%

On a member server

- %User%
- %Group%

Account Information (Windows)	The checks **Security groups and their users** and **Users and their security groups** no longer report on the ESM agent computers as users and groups.
Account Information (Windows)	The check **Security groups and their users** now correctly report the groups with the matching wildcard characters that you include in the name list.
Account Integrity (Windows)	The following checks are modified to display "None" in the **Information** field for the users who do not have a full name and "NA" for the groups who do not have a full name: ■ Allow logon through Terminal Services ■ Perform volume maintenance tasks ■ Create global objects ■ Impersonate a client for authentication **Note:** The suppressed messages reappear if you have applied any suppression that involves the Information field in an earlier SU.
Account Integrity (Windows)	The checks related to the Users rights check have been modified to enumerate the groups when you search users by using wildcards.
Active Directory (Windows Vista and Windows 2008) and Group Policy (Windows 2008)	The templates that the checks **Local Policies - Security Options** (Group Policy) and **Security options** (Active Directory) uses are now enhanced to report the User access control (UAC) related settings.
Agent Information (Windows and UNIX)	The check **ESM Application Modules** now also reports the version number of the Application module with the type of module installed.

All UNIX modules	Earlier, the modules reported an unexpected system error, if the modules could not change the locale to the locale as specified in the environment variable or as specified in the ESM_LOCALE in `/esm/config/locale.dat` file. This issue has been resolved and the modules now reports message severity as Green and message title as a Note. **Note:** The suppressed messages reappear if you have applied any suppression involving the Information field in an earlier SU.
Discovery (Windows and UNIX)	The module no longer displays unknown in the **Name** field if it is unable to obtain the DNS name for the IP. The module has been modified to report the IP address of the ESM agent computer in the **Name** field
File Attributes (Windows 2008)	The module templates are now modified to use NT SERVICE\TrustedInstaller instead of TrustedInstaller in the **Owner** column of the template.
File Attributes and File Watch (Linux)	The modules now report the correct message when you select **redhat-ia64** from the **OS** column in the **OS/REV Template Sublist Editor**.
File Find (Linux	The check **Local disk only** when enabled with the other checks no longer reports on the Network-attached storage (NAS) mounted file system.
Login Parameters (UNIX)	The module has been modified to report correct messages even if the system log file `/var/log/messages*` size is more than 1 GB.
Login Parameters (UNIX)	The check **Inactive accounts** no longer reports incorrect error messages when it parses through the sulog file.

Login Parameters (HPUX)	The checks **Warning Banners** and **Warning Banners (Check service running)** have been modified to no longer report on the HPUX 11.00 operating systems. **Note:** This check is applicable only to the ftp warning banner.
Network Integrity (UNIX)	The **TFTP** check no longer reports incorrect file name in the **Message Title** column. The check has been modified to report the correct file name tftpaccess.ctl while it verifies the Control file. **Note:** The suppressed messages reappear if you have applied any suppression involving the Information field in an earlier SU.
Object Integrity (Windows)	Earlier, the Object Integrity module used to take longer time to execute if you enabled the **Local account** check. This issue has now been resolved and the performance of the module has been drastically improved.
Object Integrity (UNIX)	The **Disk and memory access** check has been modified to report the values that you specify in the template. See "New Templates" on page 24.
OS Patches (Linux)	The module now reports an error message if unable to detect a platform or unable to retrieve a version.
Startup Files (Windows)	The **Services Security Options** check now correctly reports the SNMP service status when you select the **ACL Permissions** check box. The check now reports an exact match of the SNMP service when you use the regular expressions "^" and "$" in the System Services template. For example, ^SNMP$.

Known issue

The following issue is known in SU 2009.09.01:

Account Information, File Attributes and File Watch (Windows Vista)	The modules do not function correctly if the 'Date Modified or Date Accessed' timestamp of a file is found to be less than 1900 year. You can see the application error message in the Application log of the Event Viewer for the affected module. To resolve this issue, exclude such files from the name list or the template. Usually such files are found in `C:\Windows\winsxs` folder.