Symantec™ Critical System Protection 5.2 RU9 MP5 Release Notes

Symantec™ Critical System Protection 5.2 RU9 MP5 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: 1.0

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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, et seq."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.

Personal Information. You may configure the Licensed Software to collect personal information, including but not limited to, IP address, domain name, domain users, user name, login passwords, security logs, server logs, which is stored on Your system only and is not transmitted to Symantec. Please contact Your network administrator for further details.

Telemetry Option; Non-Personal Information. The Licensed Software contains a telemetry feature which may collect non-personal information. Such non-personal information may include, without limitation, machine configuration, SQL server details, license status, and system performance and will not be correlated with any personal information. Unless You affirmatively opt-out of this feature, telemetry will be automatically enabled to transmit such non-personal information to Symantec so we can better understand the usability and supportability of the product.

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 support 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/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/

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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support 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

Contents

Chapter 1

About Symantec Critical System Protection

This chapter includes the following topics:

- Introducing Symantec Critical System Protection
- About the documentation for Symantec Critical System Protection

Introducing Symantec Critical System Protection

Symantec Critical System Protection is a flexible, multi-layer security solution for servers that detects abnormal system activities. Symantec Critical System Protection prevents and blocks viruses and worms, hacking attacks, and zero-day vulnerability attacks. Symantec Critical System Protection also hardens systems, enforcing behavior-based security policies on clients and servers.

Symantec Critical System Protection includes a management console and server components, and agent components that enforce policies on computers. The management server and management console run on Windows operating systems. The agent runs on Windows and UNIX operating systems.

Among Symantec Critical System Protection's key features are:

- Predefined application policies for common Microsoft interactive applications
- Out-of-the-box policies that continuously lock down the operating system, high-risk applications, and databases to prevent unauthorized executables from being introduced and run
- Platform support for Microsoft Windows, Sun Solaris, IBM AIX, and Linux

Among Symantec Critical System Protection's key benefits are:

- Provides proactive, host-based security against day-zero attacks

- Offers protection against buffer overflow and memory-based attacks
- Helps to maintain compliance with security policies by providing granular control over programs and data

About the documentation for Symantec Critical System Protection

This document may be revised between releases, as new information becomes available. You can view the latest release notes and other information by clicking one of the following links:

- Symantec Critical System Protection Documentation in English
- Symantec Critical System Protection Documentation in Simplified Chinese
- Symantec Critical System Protection Documentation in Traditional Chinese
- Symantec Critical System Protection Documentation in Japanese
- Symantec Critical System Protection Documentation in Korean

Review the release notes in their entirety before you install or deploy Symantec Critical System Protection, or call for Technical Support. This document describes known issues and provides additional information that is not included in the standard documentation or the online help.

Chapter 2

New features and enhancements in this release

This chapter includes the following topics:

- Additional platform support
- Additional release information

Additional platform support

Symantec Critical System Protection Manager is now supported on Windows Server 2012 R2 (64-bit).

Symantec Critical System Protection 5.2 RU9 MP5 agents are now supported on the following platforms:

Table 2-1 Newly supported platforms

Platform	Support for IDS	Support for IPS
Red Hat Enterprise Linux 6.5 (64-bit)	Yes	Yes
Windows Server 2012 R2 (64-bit)	Yes	Yes

Additional release information

Symantec Critical System Protection now uses Apache Tomcat v7.0.52 and Java Runtime Environment (JRE) 7 Update 51.

Chapter 3

Resolved issues in this release

This chapter includes the following topics:

Prevention policy resolved issues

The following issues have been resolved in the SCSP prevention policies.

Unable to apply prevention policy due to policy translation error

Applying a prevention policy on an agent used to fail with a translation error, when the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters"** registry key was present, but the **"Working Directory"** key under it was not present.

This issue has been resolved by making the **"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Working Directory"** key optional. Now the policy is applied on the agent even if the registry key is not present.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: All Windows prevention policies

Detection policy resolved issues

The following issues have been resolved in the SCSP detection policies.

Detection events were generated even when ‘Inactive Only During the Time Interval’ rule state was selected along with the ‘Files to ignore’ option

The Windows and UNIX template policies and **My Custom Rules** of Windows and UNIX Baseline Detection policies provide an option to ignore the events that occur within a specified time frame. You can do this by configuring the **Inactive Only During the Time Interval** in **Date and time restrictions**, so that no detection events are generated during the configured period. However, detection events were still getting generated even when the **Inactive Only During the Time Interval** rule state was selected in the **Date and time restrictions** option, along with the **Files to ignore** option in the policy.

The Windows and UNIX Template policies and Detection policies in SCSP 5.2 RU9 MP5 have been modified not to generate events during the inactive period in the specific configuration.

Affected operating systems: All Windows and UNIX

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Windows and UNIX Template policies and Baseline Detection policies

Multiple detection events were being generated for the same Windows event on Windows 7 and later

Multiple detection events were being generated for the same Windows event for agents installed on Windows 7 and later. This issue occurred because the same event ID is used for multiple events, which resulted in multiple detection events being generated.

Affected operating systems: Windows 7 and later

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Windows Baseline Detection policy

Agent resolved issues

The following issues have been resolved in the SCSP agents.

SISIPS driver used to crash in a specific scenario wherein the target process was terminated before the source process could gain access

SISIPS driver used to crash in a scenario wherein a process tried to access another process by using an OpenProcess or DuplicateHandle call. This happened specifically when the target process was terminated before the source process could gain access, resulting in SISIPS driver crash.

This issue has been resolved by enhancing the SISIPS driver's process-handling capabilities.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Inbound network connections were not blocked for some processes after applying prevention policy on Windows agents

In a scenario where a listener loaded before the network filter driver was loaded, the inbound network connections were not blocked for the listener after applying prevention policy to an agent on Windows. This issue has been resolved by setting the boot-time network filters and by changing the **Start Mode** for the 'SISIPSNetFilter' kernel driver from 'Auto Start' to 'System Start'.

Affected operating systems: Windows 2008 and later

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: All Windows prevention policies

In a specific scenario, policy override tool displayed "Unknown" state after an agent upgrade, due to which policy could not be enabled

The Policy Override tool used to display "Unknown" for the **Current Policy**, **Policy Prevention**, and **Override State** fields, when the following tasks were performed in the given sequence:

- Prevention was disabled by using the override tool with self-protection enabled.

- Policy was reset to default using the Agent config tool (sisipsconfig -r).
- Agent was upgraded.
- Previously applied policy was set by using the Agent config tool (sisipsconfig -s).
- Policy override tool was launched to re-enable a policy.

Because of the "Unknown" state, it was not possible to enable the policy. Additionally, the **Extend** option also used to be disabled.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

RHEL agent reboot used to take longer than usual if the authentication server was unavailable

Rebooting the SCSP agent on RHEL used to take longer than usual if the agent used LDAP authentication and the LDAP server was down.

This issue has been resolved by modifying the SCSP driver loading scripts to ignore the user or the group name information while extracting the driver files when the authentication server is not available.

Affected operating systems: All UNIX platforms supporting IPS and RTFIM

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

SCSP 5.2.9 MP3 agent installation on RHEL used to cause an IPS service to crash

At times, installation of SCSP 5.2.9 MP3 agents on RHEL 6.0 used to cause the IPS service to crash if the PAM module used libxml2.

The zlib version 1.2.7 shipped with SCSP was incompatible with the system's libxml2.

This issue has been fixed by using the system's zlib. Shipping of zlib has been discontinued.

Affected operating systems: RHEL 5.x, 6.x

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP3, MP4

Affected Critical System Protection Policy: Not applicable

Full process paths were not being displayed for RT-FIM File Watch events on Linux

On SCSP agents installed on Linux, the full process paths were not being displayed for RT-FIM File Watch events. In the event details, the process path used to display only the name of the process and not the full path.

This issue has been fixed for most of the events. However, the issue still persists in some asynchronous file watch events.

Affected operating systems: Linux

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Installation of an SCSP agent on AIX with EMC Powerpath installed used to fail with a bosboot error

Installation of an SCSP agent on AIX used to fail with a bosboot error if the AIX machine had EMC Powerpath installed and the boot directory was EMC Symmetrix SAN device.

This issue has been fixed by modifying the bosboot command in the installer.

Affected operating systems: AIX 5.3, 6.1, and 7.1

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Event logging used to continue even after the configured disk usage limit was reached on Windows agents

At times, the value entered for **Stop logging at Disk Usage** was not honored. Events were being logged even after the specified disk usage limit was reached.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Memory leak in the IPS Service when the sub-directories in the agent log directory were missing

Instances of memory leak in the IPS Service were observed if the upload or archive directories were manually deleted, renamed, moved to another location resulting in a large number of rolled-over SCSP files.

This issue has been resolved by releasing the memory that was allocated for the logs.

Affected operating systems: All Windows and UNIX

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 or earlier

Affected Critical System Protection Policy: Not applicable

On AIX agents with network interface with IP address 0 (0.0.0.0), the network rules for a local subnet were not being enforced according to the applied policy

If a prevention policy with a network rule containing ‘LocalSubnetsIPv4only’ in the Remote IP field was applied on an AIX agent, which had one of the network interfaces in an ‘UP’ state with no IP address assigned to it, then an extra rule used to be generated. This extra rule used to be a "Match-all" rule that matched all IP addresses. In effect, instead of restricting the specified action to the IPv4 Local Subnet, the rule applied to all IPv4 addresses.

This issue has been resolved by ignoring network interfaces with IP address 0 (0.0.0.0).

Affected operating systems: AIX 6.1

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 or earlier

Affected Critical System Protection Policy: Not applicable

The ACPI-Compliant Control Method Battery device was blocked by the SCSP agent with null policy and IPS driver disabled

The power icon for battery used to disappear from the taskbar notification area and the power system icon configuration option used to be grayed out in the **Control Panel > All Control Panel Items > Notification Area Icons**, even when IPS driver was disabled and protection was not enforced.

Affected operating systems: All Windows

Affected Symantec Critical System Protection version: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Console and server resolved issues

The following issues have been resolved in the SCSP console and server.

Labels for asset groups containing a large number of agents were not being displayed in the query result

When an "Agents Registered" or a "Master Agents Registered" query was run, the query results did not display the labels of the agent groups, if the groups contained 100 or more agents. This issue has been resolved by updating the query in the report pack.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Incorrect status was being displayed for Policy Pack Status in the About dialog box

The value for the **Policy Pack Status** field in the About dialog box of the applied policy was incorrect when viewed from the **Assets** tab.

This issue has been fixed by retrieving the appropriate policy pack for the **Asset** tab.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

The "Detection Null Agent" report used to include virtual agent

The report for "Detection Null Agent" should display the native SCSP agents without any detection policy applied. However, the report used to include virtual SCSP agents along with the native agents.

This issue has been resolved by modifying the query to exclude the virtual agents from the report.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Confirmation to overwrite existing policies and configurations did not function as expected during import

In case of an import and overwrite operation for multiple policies or configurations, clicking **Yes to All** or **No to All** for the existing policies or configurations, the confirmation message used to prompt for each policy or configuration overwrite.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Incorrect count of offline agents was displayed on the Home page

The **Agent Statistics** section of the **Home** page used to display an incorrect value for the **Offline Agents** field.

This issue has been fixed by updating the query.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Editing options were grayed out in the Edit section

The **Add**, **View**, and **Remove** options to edit a policy used to be grayed out when a search string was used to search for policy content within the policy that the user wanted to edit.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Some of the right-click menu options used to gray out while switching between the tabs under Assets

Some of the right-click menu options for an asset folder used to be grayed out while switching between the **Prevention** and the **Detection** tabs under **Assets**.

Affected operating systems: All Windows

Affected Symantec Critical System Protection versions: SCSP 5.2 RU9 MP4 and earlier

Affected Critical System Protection Policy: Not applicable

Chapter 4

Known issue in this release

This chapter includes the following topics:

Agent upgrade fails on Solaris 11.1 SPARC and Solaris 11.1 x86_64

Agent upgrade fails in the following scenario:

- You have SCSP 5.2 RU9 MP4 on Solaris SPARC 11.1 or Solaris 11.1 x86_64
- You upgrade SCSP 5.2 RU9 MP4 to 5.2 RU9 MP5

Workaround: To resolve this issue, uninstall the existing version of SCSP and then install SCSP 5.2 RU9 MP5.