Symantec Critical System Protection 5.2.9 Agent Guide

Symantec Critical System Protection Agent Guide

Documentation version: 5.2.9

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 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

Agent event viewer overview

This chapter includes the following topics:

About the agent event viewer

The Symantec™ Critical System Protection agent event viewer displays recent events that were reported by your Symantec Critical System Protection agent. Events are informative, notable, and critical activities that concern your computer and Symantec Critical System Protection.

Shown as a separate, resizable window, the agent event viewer lets you see what Symantec Critical System Protection is doing on your computer.

For example, suppose you suspect that a Symantec Critical System Protection prevention policy blocked an application on your computer from working correctly. Using the agent event viewer, you can analyze the events that were reported by your agent, to determine why the application failed. Your administrator can use the results of your analysis to adjust your policy, so the application works correctly.

What you can do with the agent event viewer

You can use the agent event viewer to do the following:

- Display events reported by your Symantec Critical System Protection agent
- Display event details, including event priority, operation, process, process set, and process ID
- Sort events by column
- Search events using text strings
- Freeze and resume scrolling in the agent event viewer window
- Copy events to the Windows clipboard, for pasting into a word processing or spreadsheet document

Installing the software

The Symantec Critical System Protection agent event viewer runs on supported Microsoft Windows operating systems. The agent event viewer is automatically installed when you install the Symantec Critical System Protection agent.

See the *Symantec Critical System Protection Platform and Feature Matrix* for a list of supported operating systems.

Starting the agent event viewer

You start the Symantec Critical System Protection agent event viewer from the Windows system tray.

To start the agent event viewer

1. Log on to your agent computer.
2. Click **Start > Programs > Symantec Critical System Protection > Event Viewer**.

Chapter 2

Using the agent event viewer

This chapter includes the following topics:

Displaying events

The Symantec Critical System Protection agent event viewer lets you display events by category.

The categories are as follows:

All events	Display all prevention, detection, and management events.
Prevention	Display prevention events. An agent's prevention policy generates prevention events when applications access computer and network resources that violate the policy's behavior control.
Detection	Display detection events. An agent's detection policy generates detection events when monitored files or registry keys change, or when system or application logs generate events that match the policy's criteria.

Management	Display management events. An agent records management events that are related to the agent's configuration and communication status.
Profile	Display profile events. An agent's prevention policy generates profile events when a process is profiled.
Virtual agents	Display virtual agent events. An agent reports events from endpoint systems where Symantec Critical System Protection is not directly installed or managed.

To display events

1. In the agent event viewer, click an event category.
2. To display event details, click **View > Details**.

   Event details are shown in the bottom portion of the agent event viewer window.

Searching events

You can search events using text strings.

To search events

1. In the agent event viewer, click **Edit > Find**.
2. In the Find dialog, in the Find what box, type a text string.
3. In the Find dialog, select the search direction.
4. (Optional) In the Find dialog, select the Match case box to match uppercase and lowercase letters.
5. In the Find dialog, click **Find Next**.

Sorting events

You can sort events by column.

To sort events

- In the agent event viewer, click a column heading.

Freezing and resuming scrolling

The Freeze command lets you temporarily halt scrolling in the agent event viewer window, so that you can study the events.

To freeze and resume scrolling

1. In the event viewer, click **View > Freeze**.
2. When you are ready to resume scrolling, click **View > Resume**.

Copying events to the Windows clipboard

You can copy selected events to the Windows clipboard, and then paste the contents of the clipboard into a word processing or spreadsheet document.

The Copy as CSV command copies selected events in an unformatted style. The data items in each event are separated by commas.

The Copy command copies selected events in a formatted style.

To copy events to the Windows clipboard

1. In the agent event viewer, select one or more events.

   Press and hold the Ctrl key to select multiple events.
2. Click **Edit > Copy** or **Edit > Copy as CSV**.

Chapter 3

Using the Windows policy override tool

This chapter includes the following topics:

Starting the Windows policy override tool

You start the policy override tool from the Windows system tray.

To start the Windows policy override tool

1. Click **Start > Programs > Symantec Critical System Protection > Policy Monitor**.

   The Shield icon appears in the Windows system tray.

2. Right-click the Shield icon, and then select **Policy Override Tool**.

How to determine prevention policy enforcement status

The Shield icon indicates whether prevention policy enforcement is enabled or disabled on a Windows agent computer. Prevention policy enforcement is enabled

when an agent enforces a Symantec Critical System Protection prevention policy. When prevention policy enforcement is enabled, the Windows system tray shows the Shield icon.

When prevention policy enforcement is disabled, the Windows system tray shows the Shield icon with an X.

Prevention policy enforcement is disabled in the following situations:

- When an agent enforces the Symantec Critical System Protection Null prevention policy
- When an agent enforces the Symantec Critical System Protection Strict, Core, Limited Execution with the global disable prevention policy option enabled
- When the policy override tool is used to override prevention policy enforcement

When the prevention policy enforcement status changes, the Shield icon displays a pop-up message that notifies you of the change.

The policy override tool displays the following status information:

Agent version	The Symantec Critical System Protection agent version installed on the agent computer.
Current policy	The prevention policy applied to the agent.
Policy prevention	Indicates whether the prevention policy is enabled or disabled.
Policy override	Indicates whether your Symantec Critical System Protection administrator has allowed you to override the prevention policy.
Override state	Indicates whether the prevention policy is overridden.
Override type	The type of override that is currently enforced.
Comment	Optional comments that explain why the prevention policy was overridden, extended, or re-enabled manually.
Auto re-enable in [time]	The amount of time that remains until the prevention policy is re-enabled automatically. For example, Auto re-enable in 13 minutes 49 seconds.

Overriding prevention policy enforcement

In the Windows system tray, the Shield icon is shown with an X, to indicate that prevention policy enforcement is overridden.

Your Symantec Critical System Protection administrator must authorize you to perform each type of policy override.

To override prevention policy enforcement

1. In the policy override tool, in the Select Override Type box, select the type of policy override.
2. In the Auto re-enable after box, select an override time interval.
3. In the Enter the code box, type the random set of characters exactly as they appear.
4. (Optional) In the Comment box, explain why you are overriding the policy.

   The comments are included in the policy override event log message.
5. Click **Disable**.
6. Click **OK**.

Extending the current override time interval

You can extend the override time interval, without re-enabling and re-disabling the policy. The extended time is added to the currently remaining override time.

When extending the override time interval, you cannot change the override type. If you want to change the override type, you must re-enable the policy and then override the policy again.

To extend the current override time interval

1. In the policy override tool, in the Auto re-enable after box, select an extended time interval.
2. In the Enter the code box, type the randon set of characters exactly as they appear.
3. (Optional) In the Comment box, explain why you are extending the override time.
4. Click **Extend**.

Re-enabling prevention policy enforcement

For temporary overrides (15 minutes to 8 hours), the agent automatically re-enables the prevention policy after the override time interval expires.

You can manually re-enable the prevention policy in the following situations:

- You can manually re-enable the policy before the temporary override time interval expires.
- You can manually re-enable the policy that was overridden indefinitely.

To re-enable prevention policy enforcement

1. (Optional) In the policy override tool, in the Comments box, explain why you are re-enabling the policy.

   The comments are included in the policy override event log message.

2. Click **Re-enable**.
3. Click **OK**.

Chapter 4

Using the UNIX policy override tool

This chapter includes the following topics:

Starting the UNIX policy override tool

By default, the policy override tool is located in the following directory:

/opt/Symantec/scspagent/IPS

To start the UNIX policy override tool

1 At a command-line prompt, type and run the following command.

```
/opt/Symantec/scspagent/IPS/sisipsoverride.sh
```

2 At the Password prompt, type your UNIX login password, and then press **Enter**.

Note: Root users can list the files in /opt/Symantec/scspagent/IPS/ directory, but cannot create a new file or directory.

How to determine prevention policy enforcement status

The policy override tool displays the following status information:

Agent version	The Symantec Critical System Protection agent version that is installed on the agent computer.
Current policy	The prevention policy that is applied to the agent.
Policy prevention	Indicates whether the prevention policy is enabled or disabled.
Policy override	Indicates whether your Symantec Critical System Protection administrator has allowed you to override the prevention policy.
Override state	Indicates whether the prevention policy is overridden.
Override type	The type of override that is currently enforced.
Override user	The user who overrode the prevention policy.
Comment	Optional comments that explain why the policy was overridden, extended, or re-enabled manually.
Auto re-enable in	The amount of time that remains until the prevention policy is re-enabled automatically.

Overriding prevention policy enforcement

Your Symantec Critical System Protection administrator must authorize you to override prevention policy enforcement.

The following sample session illustrates how to override prevention policy enforcement. User-typed entries appear in bold text.

```
/opt/Symantec/scspagent/IPS/sisipsoverride.sh
Symantec Critical System Protection Policy Override


    Agent Version: 5.2.0 (build 315)
   Current Policy: sym_unix_protection_sbp, r54
Policy Prevention: Enabled
  Policy Override: Allowed
   Override State: Not overridden

To override the policy and disable protection, enter your login password.
```

```
Password: userpassword

Choose the type of override that you wish to perform:
 1. Override Prevention except for Self-Protection
 2. Override Prevention Completely
Choice? [1] 2

Choose the amount of time after which to automatically re-enable:
 1. 15 minutes
 2. 30 minutes
 3. 1 hour
 4. 2 hours
 5. 4 hours
 6. 8 hours
 7. never
Choice? [1]2

Enter a comment. Press Enter to continue.
Overriding the policy for file maintenance.

Please wait while the policy is being overridden.
.....

The policy was successfully overridden.
```

Extending the current override time interval

You can extend the current override time interval, without re-enabling and re-disabling the policy.

When extending the override time interval, you cannot change the override type. If you want to change the override type, you must re-enable the policy and then override the policy again.

The following sample session illustrates how to extend the current override time interval. User-typed entries appear in bold text.

```
/opt/Symantec/scspagent/IPS/sisipsoverride.sh
Symantec Critical System Protection Policy Override


    Agent Version: 5.2.9 (build 290)
   Current Policy: sym_unix_protection_sbp, r203
Policy Prevention: Disabled
```

```
  Policy Override: Allowed
   Override State: Overridden
    Override Type: Prevention Overridden Completely
    Override User: root
 Previous Comment: Overriding the policy for file maintenance.
Auto re-enable in: 59 minutes, 50 seconds

Do you wish to:
1. Re-enable the policy.
2. Extend the override time.
Choice? [1] 2

To extend the override time, enter your login password.
Password: userpassword

Choose the extend time:
1. 15 minutes
2. 30 minutes
3. 1 hour
4. 2 hours
5. 4 hours
6. 8 hours
7. never
Choice? [1]2

Enter a comment. Press Enter to continue.


Please wait while the override time is extended.
.....

The override time has been extended.
```

Re-enabling prevention policy enforcement

The following sample session illustrates how to re-enable prevention policy enforcement. User-typed entries appear in bold text.

```
/opt/Symantec/scspagent/IPS/sisipsoverride.sh
Symantec Critical System Protection Policy Override


    Agent Version: 5.2.0 (build 315)
```

```
   Current Policy: sym_unix_protection_sbp, r54
Policy Prevention: Disabled
  Policy Override: Allowed
   Override State: Overridden
    Override Type: Disable Prevention
    Override User: root
 Previous comment: Overriding the policy for file maintenance.
Auto re-enable in: 7 minutes, 10 seconds

Do you wish to:
1. Re-enable the policy.
2. Extend the override time.
Choice? [1] 1

Are you sure you want to re-enable the policy? (y/n) y

Enter a comment. Press Enter to continue.


Please wait while the policy is being re-enabled.
.....

The policy was successfully re-enabled.
```