Symantec Critical System Protection 5.2.9 Prevention Policy Reference Guide

Symantec Critical System Protection Prevention Policy Reference Guide

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: 5.2.9

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

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

Symantec Corporation
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

Prevention policy overview

This chapter includes the following topics:

About the prevention policies

Symantec™ Critical System Protection includes prevention policies for computers that run the following supported operating systems:

- Windows®
- Solaris™
- Linux

The Symantec Critical System Protection prevention policies protect against inappropriate modification of system resources. The policies confine each process on a computer to its normal behavior. Programs that are identified as critical to system operation are given specific behavior controls; generic behavior controls provide compatibility for other services and applications.

The Symantec Critical System Protection prevention policies typically require tailoring for your site-specific needs. For example, the base policies limit network connectivity to and from applications. If your organization requires protection beyond what the Symantec Critical System Protection prevention policies provide, you can increase or decrease the restrictions enforced by the policies. Before modifying the prevention policies, you should learn about basic and advanced policy options and how the prevention policies use process sets.

About privilege levels

The Symantec Critical System Protection prevention policies support different privilege levels. These privilege levels enable you to control processes. The prevention policies provide a starting point for protecting core OS services and a few common applications. These privilege levels provide additional means to quickly control behavior.

Note: The Windows targeted prevention policy does not support the different privilege levels.

The Symantec Critical System Protection prevention policies support the following privilege levels:

Full

Full privilege does not provide file, registry, or process restrictions. Full privilege is subject to remote network access restrictions (such as limiting which remote systems are allowed access to an agent) and network resource list restrictions. Full programs are able to bypass Symantec Critical System Protection self-protection features.

Few programs should be allowed full access.

Safe

Safe privilege is subject to Symantec Critical System Protection resource restrictions and resource list restrictions.

Any program that you do not want Symantec Critical System Protection to interfere with should be allowed safe access.

Standard

Standard (default) privilege is subject to core operating system resource restrictions, Symantec Critical System Protection resource restrictions, and resource list restrictions.

Programs that are not assigned to a specific process set (such as RPC, DNS, and IIS) or to full, safe, do not start, or custom privilege fall into this level. It is the catch-all bucket for every service or daemon that is not already identified in the policy.

This level defines what resources an application cannot modify or use. Well behaved applications should not be modifying critical system files, registry keys, or devices. Instead of adding policy controls to every application, you simply add exceptions to the default system protections already provided.

Custom

Custom privilege is subject to core operating system resource restrictions, Symantec Critical System Protection resource restrictions, and resource list restrictions.

Out of the box, there are no applications assigned to the custom bucket. You can specify applications that you want to control separately from the default bucket. For example, you may want to separately control networking, process access, buffer overflow protection, OS calls or other behavioral aspects.

Do not start

The specified program is not allowed to start. Programs running with this privilege are not allowed to access any files, registry keys, or processes. In most cases, this privilege prevents programs from starting. Programs that are still able to start are incapable of causing any harm because they are completely restricted.

About policy options

You use policy options to configure a prevention policy for assignment to a target computer. Policy options comprise a simplified set of controls that you can use to enable or disable features in a policy. Some options have associated parameters, which let you customize the behavior of an option.

The prevention policies provide policy options in a hierarchical structure. The global policy options are at the top of the hierarchy. Global policy option settings apply to all processes on a system.

The service (daemon) options and interactive program options are at the next level. The prevention policies place every process on a system into one of these two groups. The policies provide a set of options that apply to all processes in the groups. The policies also provide a set of default group options; the default option settings apply to a process that does not have specific behavior controls.

At the bottom of the hierarchy, the prevention policies provide a set of options for each service or interactive program that has specific behavior controls. Individual level option settings apply only to the specific services or programs and do not affect other services or programs in the group. Within an individual option group, the policies provide basic and advanced options.

Basic options are specific to the individual service or interactive program for which they are offered. Basic options provide configuration features specific to a service or interactive program. The prevention policies do not provide basic options for every individual program; they are only present when unique controls are necessary for a program.

Advanced policy options are standard options provided at all levels of the option hierarchy. You use advanced options to tailor prevention policies to a specific system by changing the privilege level of a service or interactive program, or by changing the control of resources by specific services or interactive programs.

Advanced options comprise the following:

- Boolean options
  - Disable prevention
  - Enable logging of trivial policy violations
  - Enable buffer overflow detection (Windows)
- Alternate privilege level
- Resource lists
- Network controls
- Process logging options

Specific options take precedence over group options, and group options take precedence over global options. For example, if a file is specified in the services resource list options as read-only, and in the resource list options of a specific service as writable, then the file is writable for the specific service because the specific option takes precedence over the group option.

How the prevention policies use process sets

The Symantec Critical System Protection prevention policies take advantage of the common characteristics of many popular services and applications. You should understand the following basic process set concepts before you apply policies to your network:

- Prevention policies divide programs into process sets, and provide behavior control to the programs based on the process set to which the program belongs.

- Each program that runs on a computer is placed in exactly one process set at any given time. These process sets are assembled into Service Options and Interactive Program Options for the streamlined administration of most policy settings.
- Most process sets and their associated behavior controls are tailored for a specific service or application. Symantec Critical System Protection takes advantage of this information by imposing very stringent behavior controls for services and applications. Only the necessary resources for each program are given read and write access privileges.
- All other services and applications are placed into the default process sets in their Service Options and Interactive Program Options groups. These default process sets use generic behavior controls that are not concerned with the allowed behavior of the services and applications, but contain behavior controls for events that should never be allowed.
- Prevention policy option hierarchy reflects the underlying process set organization of the policy. Each specific and default process set has a corresponding option group in the hierarchy. Changes to a process set's option group affect only the programs that belong to that process set. Changes that are made higher in the policy option hierarchy, such as the group or global level, affect multiple process sets.
- Policy options provide the Symantec prevention policies with the extensibility to accommodate site-specific situations that call for tighter or more forgiving behavior controls.
- Prevention policy option hierarchy (global, group, individual process set, and default process set) provides a logical grouping of process sets that you can configure to customize prevention policies.

Using the management console to learn more about policy options

To learn more about policy options, use the Symantec Critical System Protection management console in conjunction with this manual.

See the *Symantec Critical System Protection Administration Guide* for instructions on how to use the management console.

To use the management console to learn more about policy options

1. In the management console, on the **Policies** page, click **edit a policy**.
2. Navigate the policy options tree to where the controls for a specific service or interactive program are defined, and then display the option.
3. Place your mouse cursor over the option to display a description.

   For example, to learn about disabling prevention for an entire system, navigate to Global Policy Options > Disable prevention. Place your mouse cursor over the Disable prevention option to display a description.

Viewing the policy option settings

You use the management console to view a summary of the policy option settings for the prevention policies.

To view the policy option settings

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, click the **Symantec** folder.
4. In the workspace pane, double-click a Symantec Critical System Protection prevention policy.
5. In the policy dialog box, under **Policy Changes and Summary**, click **Summary**.

   A summary of the policy options is shown in tree form. The tree includes only those options that are enabled (shown in bold text) and the parameters that have values.

About custom prevention policies

A custom prevention policy is the logical equivalent of the Custom Program control. You can create, modify, and apply these custom policies separately from the prevention policies. A custom prevention policy can contain one or more custom program controls. If you create a custom prevention policy without any custom program controls, the policy is empty and you cannot apply it to a group.

Symantec Critical System Protection provides the following features for custom prevention policies:

- You can create and view the custom policies in the console policy workspace. You can add new custom policies, edit existing custom policy settings, and delete custom policies later.

- You can name custom programs more appropriately.
- You can re-use and combine custom program definitions when you apply policies.

Custom prevention policies can only be applied to groups, not directly to agents. A group can have a single primary prevention policy, and zero or more custom prevention policies applied at any given time. Custom prevention policies still depend on a prevention policy. The custom prevention policies are merged with the primary prevention policy to provide complete protection on the agent.

See "Creating a custom policy" on page 19.

Creating a custom policy

You create custom policies from the Prevention view. You can edit the policy in the New Policy Wizard or leave the policy empty and add content to it later. If a custom policy has no custom programs, then you cannot apply it to a group. Once you add at least one custom program, a blue asterisk (*) appears beside the policy name to indicate that you can apply it to a group.

Note: Each identifier that you give to a custom program that you create in a custom policy must be unique.

To create a custom policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. Under **Policy Tasks**, click **New Policy** to open the **New Policy Wizard**.
4. Type a name in the **Name** text box.
5. If you want to restrict the policy to a specific operating system, select the operating system to use the policy for.
6. If you want to select a specific policy pack to use, select it.
7. Check **Create a custom prevention policy**.
8. Click a primary policy to start from, and then click **Next**.
9. If you want to edit specific policy settings, click **Edit Policy**.
10. When you have finished making changes, click **OK**, and then click **Finish**.

See "About custom prevention policies" on page 18.

Process Access Control

This section includes the following topics:

- See "About Process Access Control" on page 20.
- See "About Process Access Control platform support" on page 20.
- See "About backward compatibility" on page 21.

About Process Access Control

Symantec Critical System Protection provides Process Access Control to enable you to control access to a running process. You can specify if a calling process can open a target process and the permissions that it has to do so.

This control has the following exceptions:

- The process accesses itself
- The process accesses one of its direct child processes

These accesses are always allowed.

The Process Access Control rules are defined in the Behavior Control Description (BCD) of the calling process. You can specify the following information:

- The target process that is accessed, including program name, user, group, and command line arguments of the target process.
- The calling process that attempts to open the target process, including program name, user, group, and command line arguments of the calling process.
- The process permissions allowed when accessing this target process. These permissions can include any combination of the individual operating system process access permissions.
- The actions to take if the permissions requested are greater than those allowed. As with file and registry access, for example, you can log or deny. These actions are similar to the actions available for file and registry accesses.

By default, the Process Access Control feature is enabled on the Symantec Critical System Protection 5.2.9 agent. To use this feature, you must have at least a 5.2.9 Prevention policy and a 5.2.9 agent.

About Process Access Control platform support

Symantec Critical System Protection supports Process Access Control on Windows, AIX, RedHat Linux, and SuSE Linux operating systems. It is supported on all

Windows operating systems with the exception of Windows 2003 (64-bit). The internal OS interfaces are not available for this control on Windows 2003 (64-bit).

Note: You cannot apply the default 5.2.9 Prevention policies on a Windows 2003 (64-bit) agent. To apply a 5.2.9 Prevention policy to a Windows 2003 (64-bit) agent, you must enable the global policy option, **Allow policy to be applied to Windows 2003 64-bit systems**, under **Additional Parameter Settings**.

About backward compatibility

Symantec Critical System Protection does not support the assignment of Process Access Control rules to agents earlier than release 5.2.9. The policies that contain Process Access Control rules are marked with a Minimum Agent Version of 5.2.9 so the console will prevent this from happening.

Policy controls

The Process Access Control rules are in the Core, Strict, Limited Execution, and Targeted Prevention policies to prevent processes from gaining write access from other processes. The default Process Access Control rule in most BCDs in these policies is configured as read-only. The Targeted Prevention policy, which is an open policy, is the exception. In the Targeted Prevention policy, the default Process Access Control rule is configured as writeable in all BCDs.

On some systems, you may need to override the default Process Access Control rule. Process Access Control lists are in the Core, Strict, Limited Execution, and Targeted Prevention policies so that you can tune them for a given system and override the default Process Access Control rule. The Process Access Control lists are available in every PSET, at the global level, at the service group level, and at the interactive program group level.

The Process Access Control lists in the policy include the following options:

- Full Access Process Access Control lists
  - Allow full access but log modifications to these processes
  - Allow full access to these processes
- Limited Access Process Access Control lists
  - Block modifications to these processes
  - Block and log modifications to these processes
- No Access Process Access Control lists

- Block all access to these processes
- Block and log all access to these processes as trivial

Precedence among Process Access Control lists

Following are the precedence rules:

- Process Access Control lists at the most specific option level take precedence.
- Within an option level, the least restrictive Process Access Control list takes precedence.
- Process Access Control lists follow the Resource list rules of precedence.

Full Privilege and Safe Privilege PSETs

The Full Privilege and Safe Privilege PSETs in the Symantec Core, Strict, and Limited Execution policies are configured with a default Process Access Control rule of writeable. You can override this rule with the Process Access Control lists for these PSETs.

In the case of Full Privilege PSETs, the policies allow all access to processes. Hence, the limited and no access resource lists only log but not block process access.

How the Symantec Critical System Protection self protection options and the Process Access Control rules interact

The Symantec Critical System Protection self protection option exists to prevent non-Symantec processes from opening Symantec Critical System Protection processes. However, there are some exceptions in the policy to allow certain processes to open Symantec Critical System Protection processes.

In the prevention policies, Process Access Control self-protection rules are first in the BCDs. Because they appear before the Process Access Control lists, you cannot use the Process Access Control lists to override the Symantec Critical System Protection self-protection. You must give a program full privileges in the policy to override the self-protection rules. This arrangement follows the same convention used for file access rules and registry access rules.

The Symantec Core, Strict, and Limited Execution policies use built-in Process Access Control rules to protect the Symantec Critical System Protection processes. The Windows and Unix Targeted Prevention policies have Symantec Critical System Protection self-protection rules that are controlled by the **Enable SCSP Self Protection** options in the policies.

Process Access Log records

The agent produces process access log records to record the process-related events. The process access events contain similar information to the existing file access and registry access IPS events.

Chapter 2

Windows prevention policy reference

This chapter includes the following topics:

About the Windows prevention policies

Symantec Critical System Protection includes the following prevention policies for computers that run Microsoft Windows operating systems:

Windows Core policy Windows Strict policy Windows Limited Execution policy	You can apply these policies to agents that run the following Windows operating systems: ■ Windows 2000 Professional/Server/Advanced Server ■ Windows Server™ 2003 Standard/Enterprise x64 ■ Windows Server 2003 Standard/Enterprise 32-bit ■ Windows 2008 ■ Windows XP Professional ■ Windows 7 Professional 32-bit and 64-bit
Windows NT® policy	You can apply this policy to agents that run Windows NT Server.

Windows Null policy	You can apply this policy to agents that run all supported Windows operating systems.
Windows Targeted Prevention policy	This policy lets you define a set of baseline controls for the entire system.

About policy options

The Windows prevention policies provide policy options in a hierarchical structure. The global policy options are at the top of the hierarchy. The service options and interactive program options are at the next level.

About global policy options

Global policy options comprise the following:

- Disable prevention
- Enable logging of trivial policy violations
- Policy override
- Resource lists
- Network controls
- Process logging options
- Profile lists
- Remote file access options
- Kernel driver options
- Host security programs
- Additional parameter settings

About service options

Services are programs that run in the background. These can be either operating system services or application server programs.

Service options affect all services on a system. Use these options to make policy changes necessary for all services.

Options for services comprise the following groups:

- Application service options allow configuration of application services for which a policy provides individual behavior controls. Application services are not part of the core operating system and are usually installed separately, after the operating system is installed.

  Application service options are provided for the following services:

  - Microsoft Exchange Server
  - Internet Information Services
  - Microsoft SQL Server

- Core OS service options allow configuration of core operating system services for which a policy provides individual behavior controls. Core OS services are installed as part of the operating system.

  Core OS service options are provided for the following services:

  - Symantec Critical System Protection agent service
  - Symantec Critical System Protection management service
  - Distributed File System
  - Distributed Transaction Coordinator
  - DNS Server
  - File Replication Service
  - License Logging Service
  - Print Spooler
  - Remote Procedure Call
  - Remote Registry Service
  - Service Control Manager
  - Secondary Logon
  - Simple TCP/IP Services
  - SNMP Service
  - Startup processes, which include smss.exe (Session Manager subsystem), csrss.exe (Client/Server Run-time Server subsystem), lsass.exe (Local Security Authority Service), and winlogon.exe (Windows Logon Process)
  - Task Scheduler Service
  - Telephony
  - Terminal Services
  - Windows Internet Name Service

  - Windows Management Instrumentation
  - Default Windows Services
- Full service options allow configuration of services with full privileges.
- Safe service options allow configuration of services with safe privileges.
- Custom service options allow configuration of custom services. These are services that you want to control separately from the default services.
- Default service options allow configuration of default services.

About interactive program options

Interactive programs are programs launched by users logged on to a system.

Options for interactive programs comprise the following groups:

- General interactive program options affect the configuration of all interactive programs on a system.
- Specific interactive program options allow configuration of interactive programs for which a policy provides individual behavior controls.

  Specific interactive program options are provided for the following services:

  - Symantec Critical System Protection UI programs
  - Microsoft Outlook and Outlook Express
  - Microsoft Office
  - Microsoft Internet Explorer
- Full interactive program options allow configuration of interactive programs with full privileges.
- Safe interactive program options allow configuration of interactive programs with save privileges.
- Custom interactive program options allow configuration of custom interactive programs. These are programs that you want to control separately from the default interactive programs.
- Default interactive programs options allow configuration of default interactive programs.

About the Windows Core prevention policy

The Windows Core prevention policy provides basic protection for the operating system and common applications, while providing a highly compatible environment for all other programs. The Core policy is suitable for most servers and workstations, and works with Windows 2000, Windows Server 2003, Windows 2008, Windows 7, and Windows XP Professional operating systems.

Policy file name: sym_win_protection_core_sbp

The Windows Core prevention policy offers the following functionality:

Privilege level

The Core policy gives safe privileges to default services and default interactive programs.

The Core policy gives safe privileges to the Windows administrators group. When a user logs on to an agent computer using an account that is a member of this group, all default interactive programs and default services that are run by this user are given safe privileges.

Interactive program protection

The Core policy provides specific behavior controls for the following interactive applications:

- Symantec Critical System Protection UI program
- Microsoft Outlook and Outlook Express
- Microsoft Office
- Microsoft Internet Explorer

Service protection

The Core policy provides specific behavior controls for the core operating system services, as well as the following application services:

- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft Internet Information Server (IIS)

The Core policy denies services from launching programs that may be used by exploits and that services normally do not launch.

Network restrictions

The Core policy prevents remote computers from making inbound network connections to an agent computer. Exception lists allow specific remote computers to make inbound network connections.

Buffer overflow detection

The Core policy enables buffer overflow detection for the following:

- Symantec AntiVirus™ and Symantec Client Security, as well as other host security programs
- Services (core OS and default)
- Interactive programs

Exception lists let you disable buffer overflow detection for specific programs.

About the Windows Strict prevention policy

The Windows Strict prevention policy provides all the protection of the Core prevention policy, and provides additional restrictions on interactive applications. The Strict policy enforces additional restrictions on interactive applications, including blocking networking, blocking modification of executable files, and treating Windows administrators as normal users. Common interactive applications work under the Strict policy, but you may need to relax the additional restrictions for some interactive programs.The Strict policy is suitable for most servers and workstations, and works with Windows 2000, Windows Server 2003, Windows 2008, Windows 7, and Windows XP Professional operating systems.

Policy file name: sym_win_protection_strict_sbp

The Windows Strict prevention policy offers the following functionality:

Privilege level	The Strict policy gives no special privileges to Windows administrators. You can use policy options to set privileged users and user groups. The Strict policy gives standard privileges to default services and default interactive programs.
Interactive program protection	The Strict policy restricts the types of e-mail attachments that can be opened. The Strict policy denies interactive programs from writing executable files on disk. This means, for example, that the policy denies downloading binaries from the Internet or saving executables sent as e-mail attachments. See Windows Core policy.
Service protection	See Windows Core policy.
Network restrictions	See Windows Core policy. The Strict policy denies network access from default services and default interactive programs, except for specific ports. This means that arbitrary programs trying to access the Internet are blocked unless specified in the exception list. The Strict policy allows outbound network connections on ports 80 (HTTP), 135 (Location Service), 389 (LDAP), and 443 (HTTPS).
Buffer overflow detection	See Windows Core policy.

The Strict prevention policy protects auto-start locations as read-only. Because many programs attempt to write to these auto-start locations in their normal operations, the following commands and functions will not work with the Strict prevention policy in place:

- The Strict policy blocks a user from running the chkdsk command and scheduling a volume to be checked on the next reboot.
- The Strict policy blocks COM object registration and ActiveX component installation.
  - The policy provides the option Block registration of COM and ActiveX controls under the Custom Interactive, Custom Service, Default Service, and Default Interactive options programs so that you can selectively allow COM Object Registration and ActiveX component installation, if necessary.
  - The following log messages are indicative of a process attempting to register a COM object or install an ActiveX component. You should clear the corresponding policy option, Block registration of COM and ActiveX controls, to allow COM object registration and ActiveX component installation if these denials are prohibiting a program from functioning correctly.

    ```
    Process: C:\Program Files\Internet
    Explorer\IEXPLORE.EXE[4232]
    Event Type: ACCESS
    Severity: WARNING
    Process Set: iexplore_ps
    Resource:
    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30528230-99F7-
    4BB4-88D8-FA1D4F56A2AB}\InprocServer32\
    Operation: NtOpenKey
    Permissions Requested: 0x20006 (set_value; create_sub_key;

     read_control)
    ```

    ```
    Process: C:\Program Files\Internet
    Explorer\IEXPLORE.EXE[4232]
    Event Type: ACCESS
    Severity: WARNING
    Process Set: iexplore_ps
    Resource: HKEY_USERS\S-1-5-21-746137067-308236825-682003330-
    70795_Classes\CLSID\{30528230-99F7-4BB4-88D8-
    FA1D4F56A2AB}\InprocServer32
    Operation: NtOpenKey
    Permissions Requested: 0x20006 (set_value; create_sub_key;
    read_control)
    ```

Note: The GUID in the Resource string is likely to change from system to system. For example: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30528230-99F7-4BB4-88D8-FA1D4F56A2AB}\InprocServer32\

- The Strict policy blocks changing network settings, such as the DNS servers.
  - Many VPN products change the DNS server setting when a tunnel is created or terminated. The policy blocks these changes, and the tunnel likely will not work. You can add the VPN program to the safe privilege list to allow software to work properly.
  - The DHCP client also changes the DNS server setting. The policy specifically allows the DHCP client to make the changes, so systems using DHCP do work with the Strict policy.
- The Strict policy blocks the ability of the system to recognize a Bluetooth device.

About the Windows Limited Execution prevention policy

The Windows Limited Execution prevention policy blocks the execution of all interactive applications, except those applications that are explicitly listed by the Symantec Critical System Protection administrator. The Limited Execution policy enforces strict restrictions on the interactive applications that are allowed to run, including blocking networking, blocking modification of executable files, and treating Windows administrators as normal users. Common applications work under this policy, but you may need to relax the strict restrictions for some interactive programs.

The Windows Limited Execution policy is suitable for dedicated workstations on which few applications are used. The policy works with Windows 2000, Windows Server 2003, Windows 2008, Windows XP Professional, and Windows 7 operating systems.

Policy file name: sym_win_protection_ltd_exec_sbp.

The Windows Limited Execution prevention policy offers the following functionality:

Privilege level	The Limited Execution policy permits only specific programs to run. The default programs that are specified in the policy as allowed to run get the same privilege as described for Strict policy.

Interactive program protection	See Windows Strict policy. The Limited Execution policy does not permit Microsoft Outlook, Outlook Express, or Microsoft Office to run.
Service protection	See Windows Core policy.
Network restrictions	See Windows Core policy.
Buffer overflow detection	See Windows Core policy.

About the Windows Null prevention policy

The Windows Null prevention policy provides no protection for an agent computer. The Null prevention policy does not log policy violations. The Null prevention policy is automatically applied to every agent when it registers with the management server. The Null policy works with all supported Windows operating systems.

Policy file name: `sym_win_null_sbp`

About the Windows Targeted prevention policy

The Targeted prevention policy lets you define a set of baseline controls for the entire system. For example, you can apply buffer overflow protection to the entire system and no other prevention. The Targeted prevention policy allows access to all resources by default and lets you block access or modifications to resources that you have configured in the policy options. It also provides you the ability to customize the policy according to your need by adding custom programs in the policy.

Policy file name: `sym_win_targeted_prevention_sbp`

See “About the Targeted prevention policy” on page 77.

Policy option descriptions

This section describes the Symantec Critical System Protection Windows prevention policies.

Boolean options

You can turn the following Boolean policy options on or off:

- Disable prevention – Log but do not prevent policy violations for the entire system
- Enable logging of trivial policy violations
- Enable buffer overflow detection

Enabling a Boolean option at a general level applies to a wider group of programs. Enabling a Boolean option at the global, group, or individual level affects a specific service or interactive program. For example, if you enable the disable prevention option at the global level, prevention is disabled for all processes, regardless of how the group level and individual level disable prevention options are configured.

Clearing the Boolean options at a general level does not supersede more specific level settings, but does allow the more specific level settings to take effect. For example, suppose you clear the disable prevention option at the global level and set it at the group level under General Service Options. Prevention is disabled for all Windows services, while interactive programs continue to prevent violations of the policy.

Disable prevention – Log but do not prevent policy violations

This option disables prevention of policy violations at the global level, service option level, interactive program option level, and pset level. At the global level, the option disables prevention of policy violations for an entire system. The violations are logged as they occur, but are not denied. Set this option to gather information about how a system performs with a policy enforced, without running the risk of Symantec Critical System Protection preventing critical system operation.

Warning: Use this option with caution. A prevention policy provides no protection when prevention is disabled.

Enable logging of trivial policy violations

A policy normally logs all policy violations. Trivial policy violations are well known, expected behaviors that violate the policy and are not critical to the operation of a program. The policy denies these behaviors. Since these denials do not represent a real security threat, the policy does not log them by default. Setting this option logs all policy violations. Note that the policy provides the same level of protection whether or not this option is set.

Warning: Turning this option on can greatly increase the size of the log files. Symantec Critical System Protection retains the same level of protection regardless of how this option is set.

Enable buffer overflow detection

Enabling this option turns on buffer overflow detection. A Symantec Critical System Protection agent can detect when applications execute code that is inserted by using buffer overflows. Note that this option is only available for certain application and core operating system services.

Policy override

This policy option gives privileges to users and user groups on an agent computer to do the following:

- Override prevention policy enforcement
  See "Override prevention completely" on page 35..
  See "Override prevention except for self-protection" on page 36..
- Install and uninstall software
  See "Override for software installation" on page 37..

Override prevention completely

This policy option lets users and user groups on an agent computer override the entire prevention policy. When the option is enabled, users can perform actions that are blocked by the prevention policy.

When the option conflicts with the self-protection option, specific naming takes precedence, and where naming is identical, the privileged option takes precedence. This lets you configure the policy to allow specific users to perform policy override while allowing all other users to perform self-protection policy override.

The policy options are as follows:

Allow all users to Disable Prevention Completely	Enable this option to allow all users on the agent computer to override the entire prevention policy. A user can re-enable prevention on the agent computer if prevention was disabled by that user.

Allow specific users to override policy enforcement	Enable this option to allow any of the listed users on the agent computer to override the entire prevention policy. In the list of users, specify the users who can perform policy override. Each entry in the list must be a user name available on the agent computer. Use of a domain name preceding the user name is permitted. A user can re-enable prevention on the agent computer if prevention was disabled by that user.
Allow specific groups to override policy enforcement	Enable this option to allow users in any of the listed groups on the agent computer to override the entire prevention policy. In the list of groups, specify the groups that can perform policy override. Each entry in the list must be a group name available on the agent computer. Use of a domain name preceding the group name is permitted. A user can re-enable prevention on the agent computer if prevention was disabled by that user.

Override prevention except for self-protection

This option lets users and user groups on an agent computer maintain Symantec Critical System Protection resource protection while overriding the prevention policy. Symantec Critical System Protection resource protection protects Symantec Critical System Protection resources, such as .ini configuration settings and log files.

The self-protection options are as follows:

Allow all users to Disable Prevention but leave SCSP Resource Protection enabled	Enable this option to allow all users on the agent computer to perform self-protection policy override. A user can re-enable prevention on the agent computer if prevention was disabled by that user.
Allow specific users to override policy enforcement	Enable this option to allow any of the listed users on the agent computer to perform self-protection policy override. In the list of users, specify the users who can perform self-protection policy override. Each entry in the list must be a user name available on the agent computer. Use of a domain name preceding the user name is permitted. A user can re-enable prevention on the agent computer if prevention was disabled by that user.

Allow specific groups to override policy enforcement	Enable this option to allow users in any of the listed groups on the agent computer to perform self-protection policy override. In the list of groups, specify the groups that can perform self-protection policy override. Each entry in the list must be a group name available on the agent computer. Use of a domain name preceding the group name is permitted. A user can re-enable prevention on the agent computer if prevention was disabled by that user.

Override for software installation

This option lets users and user groups on an agent computer install and uninstall software.

Note: This is a separate feature from the policy override feature.

The options are as follows:

Allow specific users to override policy for software installation	Enable this option to allow any of the listed users on the agent computer to install and uninstall software. In the list of users, specify the user names of the users who can perform installation override. Each entry in the list must be a user name available on the agent computer. Use of a domain name preceding the user name is permitted.
Allow specific groups to override policy for software installation	Enable this option to allow any of the listed user groups on the agent computer to install and uninstall software. In the list of groups, specify the group names of the groups that can perform installation override. Each entry in the list must be a group name available on the agent computer. Use of a domain name preceding the group name is permitted.

Resource lists

Resource lists specify files, registry keys, and processes that are writable, read-only, or blocked for both read and write. Resource lists override any controls on the same resources that are specified by the specific service or interactive program controls in a policy.

Entries in the resource lists must be full paths to files, registry keys, or processes. You may use the asterisk (*) in paths as a wildcard character. To specify an entire directory or registry tree, use an asterisk at the end of the path.

If a resource (file, registry key, process) is specified in more than one resource list, the policy applies the following general precedence rules:

- Resource lists at the most specific option level take precedence.
- Within an option level, the least restrictive resource list takes precedence.

Additional resource list precedences are as follows:

Resources added to resource lists at multiple option levels	The resource list at the most specific option level overrides the lists at the higher levels. For example, if c:\File_a is added to the read-only resource list under the Global Policy Options group and also added to the no-access resource list under the Symantec Critical System Protection Management Service group, the Symantec Critical System Protection Management service is denied access to c:\File_a, while all other processes have read-only access to c:\File_a.
Resources added to multiple resource lists at the same option level	The least restrictive resource list takes precedence. For example, if File_a is added to both the writable and read-only resource lists in the Internet Information Services option group, the Internet Information Service has write access to File_a.
Full privilege programs can access all file and registry resources	By definition, programs running with full privilege have access to all file, registry, and process resources on a computer. Full privilege settings override any restrictions placed on resources by the file, registry, and process resource lists. However, the policy does log all violations of Symantec Critical System Protection resource restrictions and of the file, registry, and process resource list settings.
Resource lists take precedence over the specifics in a behavior control description	For example, in the Internet Information Services (IIS) BCD, IIS is given write access to the following directory: systemroot%\System32\LogFiles\* If the %systemroot%\System32 directory is placed in the read-only resource list under the Internet Information Services option group, IIS cannot write its log files to the %systemroot%\System32\LogFiles directory.

Resource Lists are secondary to the built-in Symantec Critical System Protection resource restrictions

Access to the Symantec Critical System Protection resources is restricted by the prevention policies. Some of the Symantec Critical System Protection files that are installed on an agent computer and the management server computer contain sensitive information, and should not be accessed by services or applications.

These Symantec Critical System Protection files are marked as private by the policy, and access to them is denied to most services and applications. The remaining Symantec Critical System Protection resources are marked as read-only by the policy. Write access to these resources is allowed only to the Symantec Critical System Protection component that requires it.

Adding Symantec Critical System Protection resources to a resource list does not allow access to these resources. The service or application must be given full privilege by the Symantec Critical System Protection policy to access the Symantec Critical System Protection resources.

Writable resource lists

These options allow access to files, registry keys, and processes with or without logging.

The writable resource list options are as follows:

Allow but log modifications to these files

Enable this option to allow a system write access to additional files, and list the files.

The option logs file modifications.

Allow modifications to these files

Enable this option to allow a system write access to additional files, and list the files.

Allow but log modifications to these registry keys

Enable this option to allow a system write access to additional registry keys, and list the keys.

The option logs registry key modifications.

Allow modifications to these registry keys

Enable this option to allow a system write access to additional registry keys, and list the keys.

Allow full access but log modifications to these processes

Enable this option to allow a system write access to additional processes, and list the processes. The option logs process modifications.

Allow full access to these processes

Enable this option to allow a system write access to additional processes, and list the processes.

Read-only resource lists

These options allow read-only access to files, registry keys, and processes with or without logging.

The read-only resource list options are as follows:

Block modifications to these files

Enable this option to prevent a system from modifying specific files, and list the files.

Block and log modifications to these files as trivial

Enable this option to prevent a system from modifying specific files, and list the files.

The option logs violations as trivial.

Block modifications to these registry keys

Enable this option to prevent a system from modifying specific registry keys, and list the keys.

Block and log modifications to these registry keys as trivial

Enable this option to prevent a system from modifying specific registry keys, and list the keys.

The option logs violations as trivial.

Block modifications to these processes

Enable this option to prevent a system from modifying specific processes, and list the processes.

Block and log modifications to these processes as trivial

Enable this option to prevent a system from modifying specific processes, and list the processes.

This option logs violations as trivial.

No-access resource lists

These options block access to files, registry keys, and processes with or without logging.

The no-access resource list options are as follows:

Block all access to these files

Enable this option to prevent a system from accessing specific files, and list the files.

Block and log all access to these files as trivial

Enable this option to prevent a system from accessing specific files, and list the files.

The option logs violations as trivial.

Block all access to these registry keys	Enable this option to prevent a system from accessing specific registry keys, and list the keys.
Block and log all access to these registry keys	Enable this option to prevent a system from accessing specific registry keys, and list the keys. The option logs violations as trivial.
Block all access to these processes	Enable this option to prevent a system from accessing specific processes, and list the processes.
Block and log all access to these processes as trivial	Enable this option to prevent a system from accessing specific processes, and list the processes. This option logs violations as trivial.

Profile lists

This option profiles processes. Profiling records all actions taken by a process. You can use profile data to create policy controls for a process.

Note: Profiled processes are given full privileges. The prevention policies provide no protection for processes that are being profiled.

The profile options are as follows:

Profile specific processes	Enable this option to profile a process. In the list of processes, specify the full path to the process executable. You can use the asterisk (*) as a wildcard character. You can specify optional process attributes along with the full path.

The profile lists option includes process logging options. You use process logging options to configure process logging for processes that are being profiled.

See “Process logging options” on page 48..

Remote file access options

By default, programs accessing files remotely are given standard interactive program privileges. You can change the privileges given to remote programs.

The remote file access options are as follows:

Give full privileges to remote programs	Enable this option to give remote programs full privileges to access files, instead of the default standard interactive program privileges. This option removes all file and registry resource restrictions on remote programs.
Give safe privileges to remote programs	Enable this option to give remote programs safe privileges to access files, instead of the default standard interactive program privileges. This option removes the restrictions on core operating system resources given to remote programs.
Give read-only access to remote programs	Enable this option to give remote programs read-only access to all files.
Block all access from remote programs	Enable this option to block remote programs from accessing any files.

Network controls

These options control connections to and from an agent computer. The options are located throughout the policy, in general categories that cover multiple process sets, as well as within each process set.

Network controls at the global level apply to all processes on the agent computer. Network controls at the services level apply to all services on the agent computer. Network controls at the interactive program level apply to all interactive programs on the agent computer. To define exceptions for a specific service or interactive program, use the network control options specific to the service or interactive program.

The network control options comprise the following:

- The Components options define the IP addresses, TCP ports, and UDP ports that are referenced in the network rules.
- The Network Rules options define the ordered rules that control connections to and from an agent computer.
- The Default Rules options define default rule actions and log settings.

The Components options are as follows:

Components > Inbound Hosts List	These options list the IP addresses that are used in connections to and from the agent computer. Enable the options, and then list the IP addresses.

Components > Outbound Hosts List	You can list the IP addresses without using them. To use the addresses, you must reference them in a network rule.
Components > Inbound TCP Port List Components > Outbound TCP Port List	The options list TCP ports on which to block or permit requests. Enable the options, and then list the TCP ports.You can list the TCP ports without using them. To use the ports, you must reference them in a network rule.
Components > Inbound UDP Port List Components > Outbound UDP Port List	The option lists UDP ports on which to block or permit requests. Enable the options, and then list the UDP ports.You can list the UDP ports without using them. To use the ports, you must reference them in a network rule.

The Network Rules options are as follows:

Inbound Network Rules and Outbound Network Rules

Specify the network rules that control connections to and from the agent computer.

For each network rule, specify the following parameters:

- Action: Select Allow, Deny, or Disabled. The policy ignores disabled rules.
- Protocol: Select TCP, UDP, or Both TCP and UDP.
- Local Port: Type a value or select from the list.
- Remote IP: Type a value or select from the list.
- Remote Port: Type a value or select from the list.
- Logging: Select Log, Log as trivial, or Do not log.
- Program Path: Specify the full path of the program. Use of the wildcard character asterisk (*) is permitted.
- Arguments: Specify the program command-line arguments.
- User Name: Specify a user name available on the agent computer.
- Group Name: Specify a group name available on the agent computer. Use of a domain name preceding the group name is permitted.
- Rule Name: Specify an internal rule name. Rules names are carried through the system and are recorded in each event that is generated by the policy.The rule names help provide insight into why an event was recorded. You can use this information for reporting and policy adjustment purposes.
- Comment: Type a description of the rule.

See "Adding network rules" on page 45..

The Default Rule options are as follows:

Default Inbound Rule

These options define the action and log setting that are used when data does not match an enabled rule.

Default Outbound Rule

Specify the default rule action (allow, deny).

Specify the default rule log setting (Log, Log when denied, Log as trivial, Log as trivial when denied, Do not log).

The setting Log when denied only logs denials. The setting Log as trivial when denied logs as trivial for denied connections. Both settings apply to the PSET default rule options.

The following global options deny all default rules:

Globally set the default inbound rules to deny

When enabled, these options cause the policy to deny all the default rules.

Globally set the default outbound rules to deny	The options override the PSET specific and group level options.

Network control examples are provided in this guide.

See “Configuring connections to and from an agent computer” on page 88..

Adding network rules

When adding network rules, specify addresses in Classless Inter-Domain Routing (CIDR) format. A CIDR address includes an IPv4 32-bit or IPv6 128-bit IP address, plus information on how many bits are used for the network prefix. You can use the asterisk wildcard character (*) or an IP address with a netmask to indicate a range of IP addresses. For those bits not used, the corresponding bits in the IP address must be zero. For example, to match an IPv4 Class C subnet, the last octet must be zero and the mask must be 24. The IPv6 shorthand notation (::) for compressing successive zeros is not supported. Instead, use the full representation of the IP address.

Examples:

- 192.168.1.1/32 matches the IPv4 IP address exactly
- 192.168.1.0/255.255.255.0 matches an IP address with a netmask
- 10.*.*.254 and 10.160.*.85 matches IPv4 IP addresses with wildcards
- fe80:0:0:0:0:0:0:1/128 matches the IPv6 IP address exactly
- 192.168.1.0/24 matches the IPv4 Class C subnet
- fe80:0:0:0:0:0:0:0/10 matches all the IPv6 Link-Local IP addresses

Note: You can use an asterisk as one or more of the four parts of an IPv4 IP address. You cannot mix asterisks and other characters in a single octet. For example, 10.*1.*.254

Make sure you verify rule order. Network rules are ordered top to bottom. Changing the rule order changes the meaning of the rules. If you place a blocking rule before a permit rule, then the policy blocks. If you place the permit rule before the block rule, then the policy allows.

The policy ignores disabled rules.

To add network rules

1. In the management console, edit the policy.
2. In the policy editor dialog box, click **Global Policy Options > Network Controls**.

   For Inbound Network Rules, select **Inbound > Components > Inbound network rules**.

   For Outbound Network Rules, select **Outbound > Components > Outbound network rules**.
3. In the policy editor dialog box, check **List of rules to control connections into this system**, and then click **Edit[+]**.
4. In the policy editor dialog box, click **Add**.
5. In the **Entry in parameter list** dialog box, specify the rule parameters (Action, Protocol, Local Port, Remote IP, Remote Port, Logging).
6. In the **Entry in parameter list** dialog box, in the Rule Name box, type a name for the rule.
7. In the **Entry in parameter list** dialog box, in the Comment box, type a description of the rule.
8. Click **OK**.
9. Repeat the preceding steps to add another rule.
10. In the policy editor dialog box, reorder the rules if necessary.

    To reorder a selected rule, click the **blue arrows** to move the rule up or down in the list.
11. In the policy editor dialog box , click **OK**.

Kernel driver options

The kernel driver options let you to configure the kernel drivers on an agent computer.

See “Disable prevention – Log but do not prevent policy violations” on page 34..

See “Enable logging of trivial policy violations” on page 34..

See “Network controls” on page 42..

Host security programs

This policy option provides specific confinement for antivirus, spyware, firewall, and other host security programs.

The options are as follows:

Host Security Programs Installed	Symantec Critical System Protection automatically detects Symantec AntiVirus and Symantec Client Security, as well as other host security products. If you use host security programs from non-supported vendors, enable this option, and then list the programs that require host security privileges.
List of Host Security programs	List the programs that require host security privileges.

If the host security program is centrally managed, then you should configure the network controls option to allow the host security program to communicate with the manager components.

See “Network controls” on page 42..

Additional parameter settings

This option prevents programs from modifying executable files on a disk. Executable file extensions include .bat, .cmd, .com, .cpl, .dll, .exe, .hta, .js, .jse, .msc, .msi, .ocx, .pif, .ps1, .reg, .scr, .shb, .shs, .sys, .vbe, .vbs, .wsf, and .wsh.

Additional parameter settings are available at the global level and the service options level.

The options for additional parameter settings are as follows:

Enable control of modifications to executable files	Enable this option, and list the executable file extensions. See Global Policy Options > Additional Parameter Settings.
Allow specific programs to write to raw disks	Enable this option to allow specific programs to write to raw disks, such as PhyicalDrive0, and then list the programs. See Global Policy Options > Additional parameter settings.
Disable service execution of specific programs	Enable this option to specify programs that services should not execute, and list the programs. This option helps stop attacks that exploit service vulnerabilities. See Service Options > General Settings > Additional Parameter Settings.

Allow services to run these programs if using specific arguments	Enable this option to specify exceptions to the list of programs that services should not execute, and then list the programs. A restricted program is allowed to run only if its command-line arguments, user name, and group name match what is specified in the exception list. You must specify the full path of the programs. Use of the wildcard character asterisk (*) is permitted.

Process logging options

You use process logging options to configure process logging at the global level, service options level, and interactive program options level.

The options are as follows:

Log process assignment messages	Enable this option to log process assignment messages.
Log process assignment command-line arguments	Enable this option to log command-line arguments with the process assignment messages.
Log process create and destroy messages	Enable this option to log process create and destroy messages.

Enable thread injection detection

Thread injection is a technique that is used to insert and run executable code within the address space of another process. Debuggers that attach to running processes for debugging purposes often use thread injection.

This policy option addresses hostile programs that might misuse thread injection to perform a malicious task under the disguise of a benign process.

When enabled, the thread injection detection option does the following:

- Detects and reports the creation of remote threads by one process into unrelated processes.
- Takes preventive action to limit system damage caused by the injected thread while executing the injected code.
- Confines the injecting process so that it does not continue injecting threads in remote processes in the thread injection status.

Thread injection detection is enabled by default. The option is located throughout the policy.

For example:

- Process Sets > Service Options > Custom Service Options > Enable Thread Injection Detection for Custom Services
- Process Sets > Service Options > Safe Service Options > Enable Thread Injection Detection for Services with safe privileges
  An optional exceptions list is provided for disabling thread injection detection for specific services.
- Process Sets > Interactive Program Options > Custom Interactive Program Options > Enable Thread Injection Detection for Custom Interactive Programs
- Process Sets > Interactive Program Options > Safe Interactive Program Options > Enable Thread Injection Detection for Interactive Programs with safe privileges
  An optional exceptions list is provided for disabling thread injection detection for specific interactive programs.
- Advanced Options under Host Security Programs, Application Service Options, Core OS Service Options, and Specific Interactive Program Options

Alternate privilege lists/level

You use alternate privilege lists and alternate privilege levels to specify that a service or interactive program should run with a different privilege, not the privilege that it gets out of the box.

You use alternate privilege lists to list services or interactive programs that should run with a different privilege. For example, you would use Policy Settings > Service Options > Alternate Privilege Lists to list services that should have full, safe, or standard privileges, or to list services that should not run. In these generic lists, you can list services that do not have behavior controls in a policy. You can list any service running on a system.

You use alternate privilege level to set the privilege of a specific service or interactive program that already has a behavior control in a policy. For example, you would use Process Sets > Service Options > DNS Server > General Settings > Alternate Privilege Level to set the privilege level for the DNS Server, which already has a behavior control in the Windows prevention policies.

When you select an alternate privilege level for a service or interactive program, all other option settings for the service or interactive program are ignored. If you set multiple alternate privileges, the least restrictive privilege is used.

You can apply the following alternate privilege levels to a service, application, user, or user group:

- Run with full privileges
  Setting this option for a service or interactive program allows it full access to any files or registry keys on a computer. Full privilege processes are restricted however, in terms of the networking that they can perform, they obey the network remote access restrictions and the network resource lists.

  The policy logs, but does not prevent, violations of the following:

  - Symantec Critical System Protection resource restrictions
  - File and registry resource list settings

- Run with safe privileges

  Setting this option for a service or interactive program places the following restrictions on it:

  - Symantec Critical System Protection resource restrictions
  - Resource list settings

- Run with standard privileges

  Setting this option for a service or interactive program places the following restrictions on it:

  - Core OS resource restrictions
  - Symantec Critical System Protection resource restrictions
  - Resource list settings

- Do not allow to start
  Setting this option prevents a service or interactive program from starting. It does not stop processes. If the process in question is already running, you must manually stop it. Stop the process before applying the policy with this option selected. The process is given standard privileges if it remains running when the policy is applied.

When an alternate privilege level is applied to a user, all interactive applications run by that user are run at the user's privilege level. When an alternate privilege level is applied to a user group, all interactive applications run by a user in the group are run at the group's privilege level.

Option precedence

If multiple alternate privilege levels are selected for a service, application, user, or user group, the least restrictive privilege level takes precedence.

The following are exceptions to this rule:

- If the privilege level for an application differs from the privilege level of the logged-in user or group, the privilege level of the application takes precedences (for that application only). In this case, the user or group privilege level is not applied to the application.
- If an application is blocked from starting, this takes precedence over any user or group privilege settings. In this example, if a user logs in as a full privilege user, and Outlook is listed in a **Do not start** list, then the user is not allowed to start Outlook.

SysCall options

These options control privileged system calls made by services or interactive programs. These options are located in Process Sets > system_ps > General Settings > SysCall Options.

The options are as follows:

Allow mounting of file systems	Enable this option to allow custom services to mount volumes and directories.
Allow creation of hard links	Enable this option to allow custom services to create hard links.

Block registration of COM and ActiveX controls

This option prevents COM objects and ActiveX controls from registering an in-process server.

ActiveX control is a term used to denote reusable software components that are based on Microsoft's Component Object Model (COM).

Block modifications to executable files

The Windows prevention policies have options for restricting write access to executable files. This prevents unauthorized software installation on the protected system.

See Global Policy Options > Additional Parameter Settings > Enable control of modifications to executable files > List of executable file extensions for a list of file name extensions that are considered to be executables.

The option to block modifications to executable files, under specific process set option groups, determines if restrictions apply for writing executables for this process set. It is usually not recommended to disable these options, because that would allow arbitrary programs to write to executables on the disk.

Note: Alternatively, you can use the writable resource list to allow write access. When you use the writable resource list, you should be as specific as possible about the program using the resource and the resource name.

Enable this option to further confine services and interactive programs on a computer and protect against the creation of Trojan horses and many types of virus propagation.

When this option is enabled, you may not be able to copy or save executable files on the target computer, depending on the service or interactive program used and the user account used to log in to the computer.

Block modifications to startup folders

The Windows prevention policy has options for restricting write access to files under the startup folder. This prevents unauthorized launching of software as the system starts up.

The policy option to block modifications to startup folders, under a specific process set option group, determines if restrictions apply for writing to startup folders by this process set. It is usually not recommended to disable these options, because this technique is known to be used by malicious software to start itself after system restart.

Note: Alternatively, you can use the writable resource list to allow write access. When you use the writable resource list, you should be as specific as possible about the program using the resource and the resource name.

Enable this option to prevent users from modifying their startup folders. Enable this option to further confine the interactive programs on a computer and protect against the creation of Trojan horses and many types of virus propagation.

Specify services that should not start

This option defines services that should not start. Enable the option, and then list the services. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

This option does not stop processes. If the process in question is already running, you must manually stop it. Stop the process before applying the policy with this option selected. The process is given standard privileges if it remains running when the policy is applied.

Specify services with full/safe/standard privileges

This option defines services that should run with full, safe, or standard privileges. Enable the option, and then list the services. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify services with custom privileges

This option lets you separately control one or more services from the default services. Enable the option, and then list the services. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify service modules that should have no privileges

This option prevents a service module from accessing resources. Enable the option, and then list the service modules. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify service modules with full/safe/standard privileges

This option defines service modules that should run with full, safe, or standard privileges. Enable the option, and then list the service modules. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify interactive programs that should not start

This option defines interactive programs that should not start. Enable the option, and then list the interactive programs. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

This option does not stop processes. If the process in question is already running, you must manually stop it. Stop the process before applying the policy with this option selected. The process is given standard privileges if it remains running when the policy is applied.

Specify interactive programs with full/safe/standard privileges

This option defines interactive programs that should run with full, safe, or standard privileges. Enable the option, and then list the interactive programs. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify interactive program modules that should have no privileges

This option prevents an interactive program module from accessing resources. Enable the option, and then list the interactive program modules. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify interactive program modules with full/safe/standard privileges

This option defines interactive program modules that should run with full, safe, or standard privileges. Enable the option, and then list the interactive program modules. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify users with full/safe privileges

This option gives full or safe privileges to interactive programs that are run by specific users. Enable the option, and then list the users. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify groups with full/safe privileges

This option gives full or safe privileges to interactive programs that are run by users in specific groups. Enable the option, and then list the groups. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

By default, the Windows Core policy places the Administrators group in the safe privileges list.

Specify interactive programs with custom privileges

This option lets you separately control one or more interactive programs from the default interactive programs. Enable the option, and then list the interactive programs. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted. This option now is available under Process Sets > Interactive Program Options > Specific Interactive Program Options > Custom Interactive Program Options > General Settings.

SCSP agent tools

This option gives privileges to users and user groups to run the following Symantec Critical System Protection agent tools:

- sisipsconfig.exe

- Agent event viewer

See Interactive Program Options > General Settings > SCSP Agent Tools.

sisipsconfig.exe

The sisipsconfig.exe tool lets users do the following:

- Change the management server SSL certificate and password.
- Change the management server IP address and port.
- Configure disk space monitoring parameters.
- Enable or disable the state of the IPS driver.
- Manually log and profile log file rollever.
- Reset the policy to the null policy.
- Test the connection to the management server.
- View the agent settings.

Users must belong to the Administrators group to run sisipsconfig.exe.

The following options are for sisipsconfig.exe:

Allow SCSP Configuration Tools to run with full privileges for specific users

Enable this option to give full privileges to sisipsconfig.exe for specific users. The sisipsconfig.exe tool must be given full privileges or run in safe mode to function correctly. In the list of users, specify the names of the users who can run sisipsconfig.exe. Each entry in the list must be a user name available on the agent computer. Use of a domain name preceding the user name is permitted.

Allow SCSP Configuration Tools to run with full privileges for specific groups

Enable this option to give full privileges to sisipsconfig.exe for specific user groups. The sisipsconfig.exe tool must be given full privileges or run in safe mode to function correctly. In the list of user groups, specify the names of the groups that can run sisipsconfig.exe. Each entry in the list must be a group name available on the agent computer. Use of a domain name preceding the group name is permitted.

Agent event viewer

The agent event viewer is available on agent computers that run supported Windows and Windows NT Server operating systems.

See the *Symantec Critical System Protection Agent Guide* for instructions on how to use the agent event viewer.

The following options are for the agent event viewer:

Allow all users to run the SCSP Agent Event Viewer	Enable this option to allow all users on an agent computer to run the agent event viewer.
Allow specific users to run the SCSP Agent Event Viewer	Enable this option to allow any of the specifically listed users on an agent computer to run the agent event viewer. In the list of users, specify the names of the users who can run the agent event viewer. Each entry in the list must be a user name available on the agent computer. Use of a domain name preceding the user name is permitted.
Allow specific groups to run the SCSP Agent Event Viewer	Enable this option to allow any of the specifically listed user groups on an agent computer to run the agent event viewer. In the list of groups, specify the names of the groups that can run the agent event viewer. Each entry in the list must be a group name available on the agent computer. Use of a domain name preceding the group name is permitted.

Do not allow Outlook and Outlook Express to start

The Windows Limited Execution policy uses this policy option. Enable this option to prevent Microsoft Outlook and Outlook Express from starting on a computer.

The policy option does not stop programs already running. If Outlook and Outlook Express are running when you apply the policy, you must be sure to manually stop them. Once the programs are stopped, this option prevents them from restarting.

Do not allow SCSP UI programs to start

The Windows Limited Execution policy uses this policy option. Enable this option if you do not want Symantec Critical System Protection UI programs to start on a computer.

The policy option does not stop programs that are already running. If the Symantec Critical System Protection UI programs are already running when you apply the policy, you must manually stop them. Once the programs are stopped, the policy option prevents them from restarting.

Do not allow MS Office programs to start

The Windows Limited Execution policy uses this policy option. Enable this option if you do not want the Microsoft Office programs to start on a computer.

The policy option does not stop programs that are already running. If the Microsoft Office programs are already running when you apply the policy, you must manually stop them. Once the programs are stopped, the policy option prevents them from restarting.

Allow only the following programs to start

The Windows Limited Execution policy uses this policy option. Enable this option to limit users to running only selected interactive programs.

Safe privilege users are exempt from the restrictions.

The options are as follows:

Allow general system utilities to start	Enable this option to allow users to launch general system utility programs such as Windows online Help. You must specify at least one path in the list of general system utilities.
Allow specific interactive programs to start	Enable this option to allow users to launch specific programs. You must specify at least one path in the list of specific interactive programs.

About Administrator Access Control policy

The Symantec Critical System Protection prevention policies provide a mechanism to lock down administrative accounts by limiting access to programs, networks, and resources. The Symantec Critical System Protection Administrator Access Control policy lets you have an additional control over outsourced IT and remotely logged-on administrators, and against inadvertent internal access.

The feature uses generic reference lists of administrative user groups, program groups, and network groups to provide control over the administrators. After you create lists of administrative user groups, program groups, and network groups, you can then configure the policy to allow custom categories to be built based on specific combinations of these lists.

See "Accessing the generic policy reference lists" on page 57.

Accessing the generic policy reference lists

Symantec Critical System Protection prevention policies contain the following generic reference lists:

- A generic program list that contains a list of programs.
- A generic string list that contains the list of users and groups, network addresses, or network ports.

The reference lists are available when you edit the prevention policy options in the Symantec Critical System Protection console.

To access the generic policy reference lists

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. Right-click a policy, and then click **Edit Policy**.
4. In the policy editor dialog box, under **Policy Settings**, Click **MyCustom Programs**.
5. Click **+** icon to open the New Custom Control Wizard.
6. Select any of the following option from the **Category** list.

This program is interactive	Used to create an interactive program list.
This program is a Service	Used to create a service program list.
This defines a set of applications to be referenced later	Used to create a generic program lists.
This defines a list of items to be referenced later	Used to create generic string lists, which can contain user and group names, network addresses, or network ports.

See “About Administrator Access Control policy” on page 57.

See “Reference list syntax and usage” on page 58.

Reference list syntax and usage

You can create any number of reference lists, but there is no structure provided for the lists in the Symantec policies. When you use a list in other parts of the policy, be certain that you use the correct identifier. The reference list itself includes the identifier that is used to define the list itself. For example, if you have named your program list Blacklist A, it is referenced in the policy as:

```
%apps_blacklist_progs_a_list%
```

When you create a generic program list, the programs within the list can be identified using the following attributes.

Table 2-1 Program attributes

Attribute	Identifier
Program path	:prog
Arguments	:cmdline
User name	:id
Group name	:groupid

When you use a generic program list in other parts of the policy, you must include the subfield in the reference. For example, the program paths in Blacklist A are referenced in the policy using the following variable:

```
%apps_blacklist_progs_a_list:prog%
```

See "About Administrator Access Control policy" on page 57.

See "Accessing the generic policy reference lists" on page 57.

Chapter 3

UNIX prevention policy reference

This chapter includes the following topics:

- About the UNIX prevention policies
- Policy option descriptions

About the UNIX prevention policies

Symantec Critical System Protection includes the UNIX prevention policies for computers that run the following operating systems:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Sun Solaris
- VMWare Server ESX 4.1

Symantec Critical System Protection includes the following UNIX prevention policies:

UNIX Protection policy	You can apply this policy to agents that run all supported Solaris and Linux operating systems.
UNIX Null policy	You can apply this policy to agents that run all supported Solaris and Linux operating systems.
UNIX Targeted Prevention Policy	You can apply this policy to agents that run all supported Linux operating systems.

About policy options

The UNIX Protection policy provides policy options in a hierarchical structure. The global policy options are at the top of the hierarchy. The daemon options and interactive program options are at the next level.

About global policy options

Global policy options comprise the following:

- Disable prevention
- Enable logging of trivial policy violations
- Policy override
- Resource lists
- Network controls
- Process access controls
- Process logging options
- Profile lists
- NFS server access options
- NIS/NIS+ configuration

About daemon options

Daemons are programs that run in the background. These can be either operating system daemons or application server programs.

Options for daemons comprise the following groups:

- General daemon options affect all daemons on a system. Use these options to make policy changes necessary for all daemons.
- Application daemon options allow configuration of application daemons for which the policy provides individual behavior controls. Application daemons are not part of the core operating system. Application daemons are usually installed separately, after the operating system is installed.

  Application daemon options are provided for the following daemons:

  - Apache Web Server
  - Mail
  - Sendmail
  - Symantec Storage Foundation HA

- Core OS daemon options allow configuration of core operating system daemons for which a policy provides individual behavior controls. Core OS daemons are installed as part of the operating system.

  Core OS daemon options are provided for the following daemons:

  - Symantec Critical System Protection agent daemon
  - Bind daemon
  - crond daemon
  - FTP daemon
  - inet daemon
  - CUPS printer daemon
  - LPD printer daemon
  - Remote login services
  - RPC port mapper
  - Syslog daemon
  - TFTP daemon
- Full daemon options allow configuration of daemons with full privileges.
- Safe daemon options allow configuration of daemons with safe privileges.
- Custom daemon options contain options specific to custom daemons. These are daemons that you want to control separately from the default daemons. You use these options to add or remove access to specific resources for a custom daemon.
- Default daemon options allow configuration of default daemons.

About interactive program options

Interactive programs are programs launched by users logged onto a system. Interactive program options affect the configuration of all interactive programs on a system.

Options for interactive programs comprise the following groups:

- Root programs options allow configuration of programs that are run as root.
- Full interactive program options allow configuration of interactive programs with full privileges.
- Safe interactive program options allow configuration of interactive programs with safe privileges.

- Custom interactive program options contain options specific to custom interactive programs. These are interactive programs that you want to control separately from the default interactive programs. You use these options to add or remove access to specific resources for a custom interactive program.
- Default interactive program options allow configuration of default interactive programs.

About the UNIX Protection prevention policy

The Protection prevention policy provides specific behavior control descriptions for the application and core OS daemons and the specifically confined interactive programs. The remaining daemons and interactive programs are given standard privileges. The policy is suitable for most servers and workstations, and works with all supported Solaris and Linux operating systems.

UNIX policy file name: sym_unix_protection_sbp

The Protection policy offers the following functionality:

Privilege level

The root user account is the focus of confinement. Other user accounts are minimally confined, since the underlying operating system mechanisms such as file permissions already control what non-root accounts can do.

Interactive program protection

The actions of users in stdpriv, safepriv and fullpriv are mostly unconstrained by policy and mainly differ in the logging that is performed. Each of stdpriv, safepriv and fullpriv have their own resource lists.

stdpriv mimics the normal UNIX permissions by making the standard directories that contain programs such as /bin /sbin /usr/bin etc read-only.

Safe and full privileges have no specific built-in paths.

Service (daemon) protection

The Protection prevention policy provides specific behavior controls for the following core operating system daemons:

- scspagent
- bind
- crond
- ftpd
- inet
- CUPS printer daemon
- LPD printer daemon
- Remote login services
- RPC port mapper
- syslog daemon
- tftp daemon

The policy provides specific behavior controls for the following application daemons:

- apache
- mail
- sendmail
- Symantec Storage Foundation HA

Network restrictions

The policy prevents remote computers from making inbound network connections to an agent computer. Exception lists allow specific remote computers to make inbound network connections.

Standard daemons are confined to the ports they normally use.

Buffer overflow detection

Does not apply.

About the UNIX Null prevention policy

The Null prevention policy provides no protection for an agent computer. The Null prevention policy does not log policy violations. The Null prevention policy is automatically applied to every agent when it registers with the management server. The Null prevention policy works with all supported Solaris and Linux operating systems.

UNIX policy file name: sym_unix_null_sbp

Policy option descriptions

This section describes the Symantec Critical System Protection UNIX Protection policy.

Boolean options

You can turn the following Boolean policy options on or off:

- Disable prevention – Log but do not prevent policy violations for the entire system
- Enable logging of trivial policy violations

Enabling a Boolean option at a general level applies to a wider group of programs. Enabling a Boolean option at the global, group, or individual level affects a specific service or interactive program. For example, if you enable the disable prevention option at the global level, prevention is disabled for all processes, regardless of how the group level and individual level disable prevention options are configured.

Clearing the Boolean options at a general level does not supersede more specific level settings, but does allow the more specific level settings to take effect.

Disable prevention – Log but do not prevent policy violations

This option disables prevention of policy violations at the global level, daemon option level, interactive program option level, and process set level. At the global level, the option disables prevention of policy violations for an entire system. The violations are logged as they occur, but are not denied. Set this option to gather information about how a system performs with a policy enforced, without running the risk of Symantec Critical System Protection preventing critical system operation.

Warning: Use this option with caution. A prevention policy provides no protection when prevention is disabled.

Enable logging of trivial policy violations

A policy normally logs all policy violations. Trivial policy violations are well known, expected behaviors that violate the policy and are not critical to the operation of a program. The policy denies these behaviors. Since these denials do not represent a real security threat, the policy does not log them by default. Setting this option logs all policy violations. Note that the policy provides the same level of protection whether or not this option is set.

Warning: Turning this option on can greatly increase the size of the log files. Symantec Critical System Protection retains the same level of protection regardless of how this option is set.

Policy override

This policy option gives privileges to users and user groups on an agent computer to override prevention policy enforcement.

See “Override prevention completely” on page 35..

See “Override prevention except for self-protection” on page 36..

Resource lists

Resource lists specify files that are writable, read-only, or blocked for both read and write. You can use resource lists to protect specific directories and specify full paths to the files. You can use the asterisk (*) in paths as a wildcard character. To specify an entire directory, place an asterisk at the end of the path.

For writable resource lists, you can choose whether to log file modifications. For read-only and no-access resource lists, you can choose whether to log file modifications and access as trivial.

Resource lists are available at the global level, daemon option level, and interactive program option level.

If a resource (file, network port) is specified in more than one resource list, the prevention policy applies the following general precedence rules:

- Resource lists at the most specific option level take precedence.
- Within an option level, the least restrictive resource list takes precedence.

Additional resource list precedences are as follows:

- The resource list at the most specific option level overrides the lists at the higher levels.
- The least restrictive resource list takes precedence.
- Full privilege programs can access all file resources.
  By definition, programs running with full privilege have access to all file resources on a computer. Full privilege settings override any restrictions placed on resources by the file resource lists. However, the policy does log all violations of Symantec Critical System Protection resource restrictions and of the file resource list settings.
- Resource lists take precedence over the specifics in a behavior control description.
- Resource lists are secondary to the built-in Symantec Critical System Protection resource restrictions.
  The prevention policies restrict access to the Symantec Critical System Protection resources. Some of the Symantec Critical System Protection files

that are installed on an agent computer and the management server computer contain sensitive information and should not be accessed by services or applications.

The Symantec Critical System Protection files are marked as private by the policy, and access to them is denied to most daemons and applications. The remaining Symantec Critical System Protection resources are marked as read-only by the policy. Write access to these resources is allowed only to the Symantec Critical System Protection component that requires it. Adding Symantec Critical System Protection resources to a resource list does not allow access to these resources. The service or application must be given full privilege by the Symantec Critical System Protection policy to access the Symantec Critical System Protection resources.

Writable resource lists

You can allow access to files, with or without logging.

The following writable resource list options are available:

Allow but log modifications to these files	Enable this option to allow a system write access to additional files, and list the files. The option logs file modifications.
Allow modifications to these files	Enable this option to allow a system write access to additional files, and list the files.

Read-only resource lists

You can allow read-only access to files, with or without logging.

The following read-only resource list options are available:

Block modifications to these files	Enable this option to prevent a system from modifying specific files, and list the files. The option logs violations.
Block and log modifications to these files as trivial	Enable this option to prevent a system from modifying specific files, and list the files. The option logs the file modifications as trivial.

No-access resource lists

You can block access to files, with or without logging.

The following no-access resource lists are available:

Block all accesses to these files	Enable this option to prevent a system from accessing specific files, and list the files.
Block and log all access to these files as trivial	Enable this option to prevent a system from accessing specific files, and list the files. The option logs the file access as trivial.

Profile lists

This option is available under global policy options.

Profile lists comprise the following options:

- Profile specific processes
- Process logging options

Note: Process logging options are also available under daemon options and interactive program options.

Profile specific processes

This option profiles specific processes. Profiling records all actions taken by a process. You can use profile data to create policy controls for a process.

Profiled processes are given full privileges. The Protection policy provides no protection for profiled processes.

The options are as follows:

Profile specific processes	Enable this option to profile specific processes on a computer, and then list the processes. In the list of processes, you must specify the full path to each process executable. You can use the asterisk (*) as a wildcard character. You can specify optional attributes along with the full path.

Process logging options

At the global policy options level, this option configures process logging for processes that are being profiled. At the daemon options level, the option configures process logging for daemons. At the interactive program level, this option configures process logging for interactive programs.

You can enable or disable the following process logging options:

- Log process assignment messages
- Log process assignment command-line arguments
- Log process create and destroy messages

Network controls

These options control connections to and from an agent computer.

See "Network controls" on page 42..

NFS server access options

This option sets the privilege level of remote programs that access files on a target computer using NFS. By default, remote programs are placed in the default interactive program options group and given standard interactive privileges.

The NFS server access options are only available at the global policy option level.

The options are as follows:

Give full privileges to remote programs accessing files via NFS	Enable this option to give full privileges to remote programs that access files via NFS.
Give safe privileges to remote programs accessing files via NFS	Enable this option to give safe privileges to remote programs that access files via NFS.
Give read-only access to remote programs accessing files via NFS	Enable this option to give read-only access to remote programs that access files via NFS.
Block all remote file access via NFS	Enable this option to block remote programs from accessing files via NFS.

NIS/NIS+ configuration

This option lets processes on a local computer make outbound network connections to NIS/NIS+ servers.

The NIS/NIS+ configuration option is only available at the global level.

The option is as follows:

Using NIS or NIS+	Enable this option to allow processes on a local computer to make outbound network connections to specific NIS or NIS+ servers, and list the addresses. List IPV4 and IPV6 addresses if both are configured.

Alternate privilege lists/level

You use alternate privilege lists and alternate privilege levels to specify that a daemon or interactive program should run with a different privilege, not the privilege that it gets out-of-the-box.

You use alternate privilege lists to list daemons or interactive programs that should run with a different privilege. For example, you would use Daemon Options > General Settings> Alternate Privilege Lists to list daemons that should have full or safe privileges, or daemons that should not run. In these generic lists, you can list daemons that do not have individual behavior controls in a policy. You can list any daemon running on a system.

You use alternate privilege levels to set the privilege of a specific daemon or interactive program that already has an individual behavior control in a policy. For example, you would use Process Sets > Daemon Options > Core OS Daemon Options > FTP daemon > Advanced Options > Alternate Privilege Level to set the privilege level (run with full privileges, run with safe privileges, or do not start) for the FTP daemon, which already has a behavior control in the Protection policy.

When you select an alternate privilege level for a daemon or interactive program, all other option settings for that daemon or interactive program are ignored. If you set multiple alternate privileges, the least restrictive privilege is used.

Note: The Protection policy does not stop daemons or interactive programs that are already running. If a daemon or interactive program is already running when you apply a policy with the do not start option enabled, you must manually stop the daemon or interactive program. Once the daemon or interactive program is stopped, the option prevents it from restarting.

See “About privilege levels” on page 14..

Specify installation directory

This option specifies the directory in which Apache Web Server, Mail, and Sendmail were installed. The option also specifies the path for the Apache logs. Default directories are supplied.

See the following policy options:

- Process Sets > Daemon Options > Application Daemon Options > Apache Web Server > Basic Options > Specify installation directory
- Process Sets > Daemon Options > Application Daemon Options > Apache Web Server > Basic Options > Apache log path
- Process Sets > Daemon Options > Application Daemon Options > Symantec Storage Foundation HA > Basic Options > Specify installation directory

The options are as follows:

Specify installation directory	If you installed Apache Web Server or Symantec Storage Foundation HA in a different directory, enable this option, and then replace the old installation directory path with the new directory path.
Apache log path	Enable this option to specify the path for the Apache logs, and list the path.

SysCall options

These options control privileged system calls made by full, safe, and standard privilege daemons.

See “About privilege levels” on page 14..

The options are available at the daemon options level and interactive programs option levels.

The options are as follows:

Allow mounting and unmounting of file systems	Enable this option to allow full, safe, and standard privilege daemons to mount and unmount file systems.
Allow mounting to these mountpoints only	Enable this option to allow full, safe, and standard privilege daemons to mount file systems only at specific mountpoints. List the mountpoints that the daemons can mount to and unmount from.
Allow creation of hard links	Enable this option to allow full, safe, and standard privilege daemons to create hard links.

Allow creation of special files	Enable this option to allow full, safe, and standard privilege daemons to create FIFO, block, or character special files.
Allow loading and unloading of kernel modules	Enable this option to allow full, safe, and standard privilege daemons to load and unload kernel modules.

Terminal emulation programs supported

This option lists the terminal emulation programs used on a computer. This routes processes and child processes to the appropriate interactive process set.

This option is available at the interactive program options level.

See Interactive Program Options > General Settings > Terminal emulation programs supported.

The option is as follows:

Terminal emulation programs supported	Enable this option to specify the terminal emulation programs used on a computer, and list the terminal emulation programs.

System admin options

These options control which system administration options are allowed.

See Process Sets > Interactive Program Options > Specific Interactive Program Options > Root Program Options > System Admin Options.

The options are as follows:

Allow root to run the useradd program	Enable this option to allow the root user to run the useradd program with safe privilege.
Allow access to disk devices	Enable this option to execute file system maintenance commands such as fdisk and fsck.
Allow tools such as truss and gcore to access process data	Enable this option to allow diagnostic programs to access process data via the /proc file system. This access is needed by programs such as truss, gcore, and pfiles.

SCSP configuration tool options

This option controls whether the root user can run the su command to become the sisips user. The Protection policy allows the sisips user to run the sisipsconfig.exe tool, which can be used for many purposes including disabling prevention.

This option is available at the interactive program options level.

See Process Sets > Interactive Program Options > Specific Interactive Program Options > Root Program Options > SCSP Configuration Tool Options.

The option is as follows:

Allow SCSP configuration tools to run with full privileges for the root user	Enable this option to become the sisips user. The option is disabled by default. When the option is disabled, the root user cannot become the sisips user.

Specify daemons that should not start

This option defines daemons that should not start. Enable the option, and then list the daemons. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

This option does not stop processes. If the process in question is already running, you must manually stop it. Stop the process before applying the policy with this option selected. The process is given standard privileges if it remains running when the policy is applied.

Specify daemons with full/safe privileges

This option defines daemons that should run with full or safe privileges. Enable the option, and then list the daemons. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify daemons with custom privileges

This option lets you separately control one or more daemons from the default daemons. Enable the option, and then list the daemons. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify interactive programs that should not start

This option defines interactive programs that should not start. Enable the option, and then list the interactive programs. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

This option does not stop processes. If the process in question is already running, you must manually stop it. Stop the process before applying the policy with this option selected. The process is given standard privileges if it remains running when the policy is applied.

Specify interactive programs with full/safe/standard privileges

This option defines interactive programs that should run with full, safe, or standard privileges. Enable the option, and then list the interactive programs. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify interactive programs with custom privileges

This option lets you separately control one or more interactive programs from the default interactive programs. Enable the option, and then list the interactive programs. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify users with full/safe privileges

This option gives full or safe privileges to interactive programs that are run by specific users. Enable the option, and then list the users. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Specify groups with full/safe privileges

This option gives full or safe privileges to interactive programs that are run by users in specific groups. Enable the option, and then list the groups. Each entry in the list must be a full path. Use of an asterisk (*) as a wildcard character is permitted.

Targeted prevention policy

This chapter includes the following topics:

About the Targeted prevention policy

The Targeted prevention policy lets you define a set of baseline controls for the entire system. For example, you can apply buffer overflow protection to the entire system and no other prevention.

The Targeted prevention policy allows access to all resources by default and lets you block access or modifications to resources that you have configured in the policy options. It also provides you the ability to customize the policy according to your need by adding custom programs in the policy.

Policy file name for Windows operating systems: `sym_win_targeted_prevention_sbp`

Policy file name for UNIX operating systems: `sym_unix_targeted_prevention_sbp`

The Targeted prevention policy includes an SCSP self protection option. When the SCSP self protection option is selected, it protects against a user or a process tampering with the Symantec Critical System Protection configuration data or program data.

For example, the following configuration data is protected as the write access is blocked and logged whereas the read access is blocked but not logged:

- The Certificate files on server, console, and agent
- The server configuration file `tomcat\conf\server.xml`
- The IPS agent configuration file `IPS\agent.ini`
- The IDS agent configuration file `IDS\agent.ini`

The following configuration data and program data is protected as read-only:

- All files under the agent install directory
- All files under the agent log directory
- All Symantec Critical System Protection driver files

The following directories are protected against being renamed:

- The agent install directory
- The agent log directory

The Targeted prevention policy provides the following options:

Global Policy options	Provides a set of global options that applies to all the processes on the system. When you apply global options in the policy, they are applied to all the PSETs in the policy.
Built-In PSET options	Provides a set of options to configure the Built-In PSETs. The Windows Targeted prevention policy contains four built-in PSETs to handle Kernel Driver controls, Remote File Access controls, Symantec Critical System Protection Agent and Server controls. The Targeted prevention policy always routes these processes to the built-in PSETs. You cannot override these built-in PSETs.
Default PSET options	The Targeted prevention policy routes all processes to the Default PSET with the exception of Built-In PSETs. You can configure all protection features in the Default PSET.
My Custom Programs	Define one or more custom program within the policy to override the security settings in the Default PSET. Additionally, you can also define custom lists which can be referenced elsewhere in the policy.

Note: If you set Disable Prevention at a global level, then Symantec Critical System Protection disables prevention for all PSETs. You cannot enable prevention in a Custom PSET or a Default PSET.

See "How the Targeted prevention policy works" on page 79.

See "About using custom lists with the Targeted prevention policy" on page 81.

See "About using custom programs with the Targeted prevention policy" on page 79.

How the Targeted prevention policy works

The Targeted prevention policy includes a set of Built-In PSETs to control access to the kernel and Symantec Critical System Protection processes. You cannot override a Built-In PSET. However, you can configure the Built-In PSETs by using the policy options.

With the exception of the Built-in PSETs, the Targeted prevention policy routes all processes to the Default PSET. All protection features are configurable in the Default PSET. However, the Default PSET can be overridden by adding a custom program to the policy. One or more custom programs can be defined within the policy which will override the security settings in the Default PSET.

See "About the Targeted prevention policy" on page 77.

See "About using custom lists with the Targeted prevention policy" on page 81.

See "About using custom programs with the Targeted prevention policy" on page 79.

About using custom programs with the Targeted prevention policy

The Targeted prevention policy lets you create custom programs based on the following templates:

Fully open template	Use the fully open custom program template to build-up security protections. By default, it has no security restrictions. All processes assigned to the fully open custom program have no default resource restriction defined. Moreover, protection features such as buffer overflow detection, thread injection are also disabled. See "Creating custom programs based on the fully open template" on page 82.

Fully closed template

Use the fully closed custom program template to relax security protections. All processes assigned to the fully closed custom program are denied access to all resources and all protection features are enabled by default. The protection features such as buffer overflow detection, thread injection are also enabled by default.

See “About using the fully closed custom program template” on page 80.

See “Creating custom programs based on the fully closed template” on page 83.

See “About using custom lists with the Targeted prevention policy” on page 81.

See “About the Targeted prevention policy” on page 77.

About using the fully closed custom program template

You can use the fully closed custom program template in the following ways:

- If you do not want a program to run at all, then you can create a fully closed custom program and route the program to this custom program PSET.

  Note: This method does allow the program to run, although the program is blocked from accessing any file, registry, or network resources.

- If you want to strictly limit a program regarding the resources it can access, you can create a fully closed custom program. You must configure the custom program and allow write access to only the resources this program needs access to, while allowing read access to all resources on the system.

By default, the fully closed custom program denies access to all resources and logs all access attempts as trivial. Since, all access attempts are logged as trivial, you can enable trivial logging for this custom program to see what resources the program attempts to access.

Symantec recommends you to configure the custom program to allow read access to all resources on the system, and to only allow write access to the resources as required by this custom program.

To determine what resources the custom program needs write access to

1. Edit the file, registry, and process access rules in the custom program and place a wildcard in the Read-only Resource Lists:

   - Block modifications to these files

- Block modifications to these Registry keys

2. Enable logging of trivial policy violations in the custom program under General Settings.
3. Disable prevention in the custom program.

Apply this policy to the agent, and then execute the custom program. The trivial events generated will show what resources the program is accessing for write access. You can use these events to configure the custom program and allow write access to the appropriate resources. Once you have determined the specific resources the program needs write access to, you can then enable the prevention in the custom program.

See "About using custom programs with the Targeted prevention policy" on page 79.

See "Creating custom programs based on the fully closed template" on page 83.

About using custom lists with the Targeted prevention policy

The Targeted prevention policy lets you create generic program lists and generic string lists. You can refer to these custom lists in other parts of the policy. You can access these custom lists by editing the Targeted prevention policy in the management console.

Generic Program list	The generic program list contains a list of programs. In the management console, the generic program list appears as set of applications to be referenced later.
Generic String list	The generic string list contains a list of users, groups, network addresses, or network ports. In the management console, the generic string list appears as list of items to be referenced later.

See "About using custom programs with the Targeted prevention policy" on page 79.

See "About the Targeted prevention policy" on page 77.

Creating custom programs based on the fully open template

The Symantec Critical System Protection Targeted prevention policy lets you create custom programs based on the fully open template.

To create a custom program based on the fully open template

1. In the management console, click **Prevention View**.
2. On the **Policies** page, click the **Symantec** folder and then in the workspace pane, double-click **sym_win_targeted_prevention_sbp**.
3. In the policy editor dialog box, click **My Custom Programs**, and then click **New**.
4. In the **New Custom Control Wizard** dialog box, specify the following information:

Display Name	Type a descriptive name. Example: Notepad
Category	Select **This Custom Program PSET is fully open, it has no default security restrictions**.
Identifier	Type a unique name that the policy uses internally. The identifier must not include spaces or special characters. Example: NotepadID
Description	Type a full description.

5. Click **Finish**.
6. In the policy editor dialog box, click **My Custom Programs > Notepad > Settings**.
7. In the **Notepad Settings** pane, double-click **Notepad[cust_NotepadID_ps]** and do the following:
   - Check and expand **This Custom Program PSET is fully open, it has no default security restrictions**, and then click **List of programs to route to this custom PSET**.
   - In the **List of programs to route to this custom PSET** section, click **Add**, and then add the following path:
     C:\Windows\system32\notepad.exe
   - Check **Enable SCSP Self Protection**.

8 In the policy editor dialog box, double-click **File Rules**> **Read-Only Resource Lists** and do the following:

- Check and expand **Block modifications to these files**, and then click **List of files that should not be modified**.
- In the **List of files that should not be modified** section, click **Add**, and then add the file path that you do not want to be modified. For example, test.txt.

9 Click **OK** and apply the policy on the agent.

10 On the agent computer, open the test.txt file and verify the following events:

The Notepad.exe getting assigned to the custom pset cust_NotepadID_ps	PPST,655,2011-09-09 20:02:38.919 Z-0400 ,I,,,b3218cab450cde2dde92d225489f4ee0, e,,,WIN2K8-R2\Administrator,0,C:\Windows\system32\NOTEPAD.EXE,3844,,"& quot 1;C:\Windows\system32\NOTEPAD.EXE & quot 1 C:\temp\test.txt",create,cust_NotepadID_ps, 2360,,,,C:\Windows\Explorer.EXE,,,\WINDOWS\SYSTEM32\SHLWAPI.DLL,3464,,
Denied File Access Event when the test.txt is accessed by using notepad	PFIL,656,2011-09-09 20:02:38.593 Z-0400, W,,R,b3218cab450cde2dde92d225 489f4ee0,e,,,WIN2K8-R2\Administrator,0,C:\Windows\system32\NOTEPAD.EXE,3844,D, C:\temp\test.txt,NtCreateFile, cust_notepad_ps, ffffffff,c0000022, 00120089,,,,00000001,\WINDOWS\SYSTEM32\KERNELBASE.DLL,3464,,

See “About using custom programs with the Targeted prevention policy” on page 79.

See “Creating custom programs based on the fully closed template” on page 83.

Creating custom programs based on the fully closed template

The Symantec Critical System Protection Targeted prevention policy lets you create custom programs based on the fully closed template.

To create a custom program based on the fully closed template

1. In the management console, click **Prevention View**.
2. On the **Policies** page, click the **Symantec** folder and then in the workspace pane, double-click **sym_win_targeted_prevention_sbp**.
3. In the policy editor dialog box, click **My Custom Programs**, and then click **New**.
4. In the **New Custom Control Wizard** dialog box, specify the following information:

Display Name	Type a descriptive name. Example: Services
Category	Select **This Custom Program PSET is fully closed and locked down by default**.
Identifier	Type a name that the policy uses internally. Example: Services
Description	Type a full description.

5. Click **Finish**.
6. In the policy editor dialog box, check **Services[cust_Services_ps]**, and do the following:
   - Check and expand **This Custom Program is fully closed and locked down by default**, and then click **List of programs to route to this custom PSET**.
   - In the **List of programs to route to this custom PSET** section, click **Add**, add the following path:
     C:\Windows\system32\tlntsvr.exe
   - Check **Child processes remain in this custom PSET**.
   - Check **Enable Buffer Overflow Protection**.
   - Check **Enable Thread Injection Detection**.
7. Click **OK** and apply the policy on the agent.
8. Open the log file from the following path:

   C:\Program File(x86)\Symantec\Critical System Protection\Agent\IPS\scsplog
9. Verify that tlntsvr.exe is routed to the defined Custom PSET, cust_Services_ps and remaining processes are routed to the Default PSET.

See “Creating custom programs based on the fully open template” on page 82.

See “About using the fully closed custom program template” on page 80.

See “About using custom programs with the Targeted prevention policy” on page 79.

Chapter 5

Policy examples

This chapter includes the following topics:

Configuring connections to and from an agent computer

The following examples illustrate how to use the Network Controls option.

Blocking inbound network connections from known IP addresses

To restrict specific IP addresses from making inbound connections to an agent computer, you block the inbound connection to any program listening on a potential target port.

Make sure you modify the policy settings in the global section of the policy. Because global rules are always evaluated after group and specific rules, the denials will hold only if there are no contradicting group or specific rules. For example, a network rule for the DNS service that is specified under the DNS process set options and allows inbound connections from all IP addresses on the DNS port will allow a bad IP address to make inbound connection on the DNS port even though it is denied in the global options.

To block inbound network connections from known IP addresses

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Global Policy Options > General Settings > Network Controls > Inbound**, check **Inbound network rules** and then click **Edit[+]**.
6. In the policy editor dialg box, under **List of rules to control connections into this system**, click **Add**.
7. Specify the following rule parameters:

Action	Select **Deny**.
Protocol	Select **Both TCP and UDP**.
Remote IP	Specify the remote IP address.
Logging	Select **Log** to log an event when a connection attempt is blocked.

8 Click **OK**.

9 Re-order the list of rules if necessary.

10 In the policy editor dialog box, click **OK**.

11 Apply or reapply the policy to the agent.

Restricting client connections to dedicated servers

You can restrict network connections of a specific protocol to exist only between a server and its intended clients.

Allowing remote connections from all remote IP addresses to a specific server

On the server, it is always best to define network protection using the specific process set options (for example, dns_ps). This ensures that only the intended service or program may accept requests on the dedicated port. Specifying IP addresses of clients ensures that only authorized clients are allowed to send requests to the server.

To allow remote connections from all remote IP addresses to a specific server:

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a prevention policy, and then right-click **Edit Policy**.

5 n the policy editor dialog box, under **Global Policy Options > General Settings > Network Controls > Outbound**, check **Outbound network rules** and then click **Edit[+]**.

6 In the policy editor dialg box, under **List of rules to control outbound network connections**, click **Add**.

7 Specify the following rule parameters:

Action	Select Allow.
Protocol	Select the protocol.
Remote IP	Specify the server IP address.
Remote Port	Specify the service port.
Logging	Select a logging option.

8 Click **OK**.

9 Re-order the list of rules if necessary.

10 In the policy editor dialog box, click **OK**.

11 Apply or reapply the policy to the agent.

Allowing connections from specific clients to the DNS server

On the client, the policy can specify the service port, protocol, and server IP address. Define a rule in the global option group if access to the service is required by many services and interactive programs. Define the rule in the appropriate process set network options if the service is required by a limited number of services and interactive programs. Granular rules provide better protection. Restricting an outbound connection to a known set of programs may provide protection from spyware trying to use a well known port so it seems benign on the network.

To allow connections from specific clients to the DNS service:

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Process Sets**.

6 In the policy editor dialog box, under **Process Sets > Service Options >Core OS Service Options**, click **Edit[+]** before **DNS Server[dns_ps]**.

7 In the policy editor dialog box, under **DNS Server[dns_ps] > General Settings > Network Controls > Inbound**, check **Inbound network rules** and then click **Edit[+]**.

8 In the policy editor dialog box, under **List of rules to control connections into this system**, click **Add**.

9 Specify the following rule parameters:

Action	Select **Allow**.
Protocol	Select the protocol.
Local Port	Specify the DNS port.
Remote IP	Specify the IP address. Use the CIDR notation to define an IP range or use the pre-defined component options.
Remote Port	Specify the remote port.
Logging	Select **Log**.

10 Click **OK**.

11 Re-order the list of rules if necessary.

12 In the policy editor dialog box, under **DNS Server[dns_ps] > General Settings > Network Controls > Inbound**, click **Edit[+]** before **Default inbound rule** and specify the following:

Default inbound rule action	Select **Deny**.
Default inbound rule log setting	Select **Log**.

13 In the policy editor, click **OK**.

14 Apply or reapply the policy to the agent.

Configuring Outlook and Outlook Express

The Symantec Critical System Protection Windows prevention policies can restrict which programs can be opened as attachments from Outlook and Outlook Express. By default, the Strict prevention policy restricts email attachment opening to text files, .pdf files, .zip files, and Microsoft Office documents.

Allowing a specific program to be executed

You can add additional programs to be executed from Outlook and Outlook Express.

To allow a specific program to be executed from Outlook or Outlook Express, and open an email attachment

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Process Sets**.
6. In the policy editor dialog box, under **Process Sets > Interactive Program Options > Specific Interactive Program Options**, click **Edit[+]** before **Outlook and Outlook Express[outlook_ps, int_mailchild_ps, int_mailchild_unsafe_ps]**.
7. In the policy editor dialog box, under **General Settings > Basic Options**, check **Enable opening of specific email attachments** and then click **Edit[+]**.
8. In the policy editor dialog box, under **The list of email attachment programs allowed to execute**, click **Add**, and then add the program path and name to the list of email attachment programs allowed to execute.
9. Click **OK** to save your changes.
10. Apply or reapply the policy to the agent.

Disabling the opening of all email attachments

You can disable opening attachments.

To disable the opening of all email attachments

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Process Sets**.
6. In the policy editor dialog box, under **Process Sets > Interactive Program Options > Specific Interactive Program Options**, click **Edit[+]** before **Outlook and Outlook Express[outlook_ps, int_mailchild_ps, int_mailchild_unsafe_ps]**.

7 In the policy editor dialog box, under **General Settings > Basic Options** , uncheck **Enable opening of Microsoft Office email attachments** and **Enable opening of specific email attachments**.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving interactive programs full or safe privileges

If an interactive program does not have specific behavior controls written for it, the Windows prevention policies give it standard privileges. Programs that have standard privileges are subject to the Core operating system resource restrictions, Symantec Critical System Protection resource restrictions, and the user-defined resource list settings.

Some programs require access to these resources to function correctly. You can grant this access by giving these programs full or safe privileges within the policy.

By default, the following programs are given safe privileges within all of the prevention policies:

- Antivirus programs
- Microsoft Systems Management Server (SMS) client programs

Giving interactive programs full privileges

Programs that have full privileges are not subject to file or registry restrictions.

To give interactive programs full privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > Alternate Privilege Lists**, check **Specify Interactive Programs with Full Privileges** and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of Interactive Programs with Full Privileges**, click **Add**, and then add the program to the list of interactive programs with full privileges. .

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving interactive programs safe privileges

Programs that have safe privileges are subject to the Symantec Critical System Protection resource restrictions and the user-defined resource list settings.

To give interactive programs safe privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > Alternate Privilege Lists**, check **Specify Interactive Programs with Safe Privileges** and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of Interactive Programs with Safe Privileges**, click **Add**, and then add the program to the list of interactive programs with safe privileges.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving services full or safe privileges

You can give a service additional privileges.

Giving services full privileges

You can give services full privileges.

To give services full privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Service Options**.
6. In the policy editor dialog box, under **Service Options > General Settings > Alternate Privilege Lists**, check **Specify Services with Full Privileges** and then click **Edit[+]**.
7. In the policy editor dialog box, under **List of Services with Full Privileges**, click **Add**, and then add the program to the list of services with full privileges.
8. Click **OK** to save your changes.
9. Apply or reapply the policy to the agent.

Giving services safe privileges

You can give services safe privileges.

To give services safe privileges

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Service Options**.
6. In the policy editor dialog box, under **Service Options > General Settings > Alternate Privilege Lists**, check **Specify Services with Safe Privileges** and then click **Edit[+]**.
7. In the policy editor dialog box, under **List of Services with Safe Privileges**, click **Add**, and then add the program to the list of services with safe privileges.
8. Click **OK** to save your changes.
9. Apply or reapply the policy to the agent.

Giving users policy override privileges

You can allow users to override a prevention policy on an agent computer so they can perform blocked actions such as accessing files and networks.

To give users policy override privileges

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Global Policy Options**.
6. In the policy editor dialog box, under **Global Policy Options > General Settings > Policy Override**, check the desired policy override options.

   See "Policy override" on page 35..

   See "Policy override" on page 67..
7. Click **OK**.
8. Apply or reapply the policy to the agent.

Overriding prevention policy enforcement

Users who are allowed to override a prevention policy on an agent computer can do so by using the policy override tool. The tool is available on agent computers that run supported Windows, Solaris, and Linux operating systems.

Users can use the policy override tool to do the following:

- Display the name of the prevention policy that is applied to the agent.
- Determine whether prevention policy enforcement is enabled or disabled.
- Determine whether they are allowed to override the prevention policy.
- Override the prevention policy.
- Re-enable the prevention policy.
- Display how much time remains until the prevention policy is re-enabled automatically.
- Extend the policy override time.

Giving users install and uninstall privileges

You can allow specific users and user groups on a Windows agent computer to install and uninstall software.

To give users install and uninstall privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Global Policy Options**.

6 In the policy editor dialog box, under **Global Policy Options > General Settings > Policy Override > Override for software installation**, check the desired options.

  See "Override for software installation" on page 37.

7 Click **OK**.

8 Apply or reapply the policy to the agent.

Giving users and user groups additional privileges

When an alternate privilege level is applied to a user, all interactive programs run by that user are run at the user's privilege level. When an alternate privilege level is applied to a user group, all interactive programs run by a group member run at the group's privilege level.

Giving users full privileges

You can give users full privileges.

To give users full privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > Alternate Privilege Lists**, check **Specify users with full privileges** and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of users with full privileges**, click **Add**, and then add the users to the list of users with full privileges.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving users safe privileges

You can give users safe privileges.

To give users safe privileges

1 In the management console, click **policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > Alternate Privilege Lists**, check **Specify users with safe privileges** and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of users with safe privileges**, click **Add**, and then add the users to the list of users with safe privileges.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving user groups full privileges

You can give user groups full privileges.

To give user groups full privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > Alternate Privilege Lists**, check **Specify groups with full privileges** and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of groups with full privileges**, click **Add**, and then add the groups to the list of groups with full privileges.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving user groups safe privileges

You can give user groups safe privileges.

To give user groups safe privileges

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > Alternate Privilege Lists**, check **Specify groups with safe privileges** and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of groups with safe privileges**, click **Add**, and then add the groups to the list of groups with safe privileges.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Configuring prevention in a policy

When initially configuring one or more computers in a production environment, enable the global disable prevention option. This option disables the prevention of Symantec Critical System Protection policy violations for the entire system. The violations are logged as they occur, but are not denied. This configuration lets you gather information about how a computer performs with a specific policy, without running the risk of Symantec Critical System Protection preventing critical computer operations.

After the Windows prevention policy is applied, exercise the computer and all applications. Exercise includes, but is not limited to, the following:

- Periodic maintenance activities
- System backups
- Restarting the computer to ensure the system services and applications are able to start up properly
- Virus scans
- Updates of virus definitions used by antivirus software

Examine log messages produced by these activities and modify the policy configuration as necessary to allow the computer to operate properly. Once you verify that the computer operates properly with the policy, clear the global disable prevention option.

To configure prevention in a policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Global Policy Options**.
6. In the policy editor dialog box, under **Global Policy Options > General Settings**, check or uncheck **Disable prevention – log but do not prevent policy violations for the entire system**.
7. Click **OK** to save your changes.
8. Apply or reapply the policy to the agent.

Giving privileges to run sisipsconfig.exe

The Symantec Critical System Protection agent includes the command-line tool sisipsconfig.exe. This tool reconfigures parameters that are set during installation and parameters that are not currently accessible with the management console.

Because the Symantec Critical System Protection Windows prevention policies include protection against processes that modify Symantec Critical System Protection resources, users cannot run sisipsconfig.exe with the default policy settings.

As the administrator, you can give full privileges to sisipsconfig.exe for specific users and user groups. To do this, you must configure the sisipsconfig.exe options in the Windows prevention policies.

Giving full privileges to sisipsconfig.exe for specific users

You can give full privileges to sisipsconfig.exe for specific users.

To give full privileges to sisipsconfig.exe for specific users

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.
6. In the policy editor dialog box, under **Interactive Program Options > General Settings > SCSP Agent Tools**, check **Allow SCSP Configuration Tools to run with full privileges for specific users**, and then click **Edit[+]**.
7. In the policy editor dialog box, under **List of users allowed to run the SCSP configuration tools with full privileges**, click **Add**, and then add the user names to the list of users allowed to run sisipsconfig.exe with full privileges.
8. Click **OK** to save your changes.
9. Apply or reapply the policy to the agent.

Giving full privileges to sisipsconfig.exe for specific groups

You can give full privileges to sisipsconfig.exe for specific groups.

To give full privileges to sisipsconfig.exe for specific groups

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > SCSP Agent Tools**, check **Allow SCSP Configuration Tools to run with full privileges for specific groups**, and then click **Edit[+]**.

7 In the policy editor dialog box, under **List of groups allowed to run the SCSP configuration tools with full privileges**, click **Add**, and then add the group names to the list of groups allowed to run sisipsconfig.exe with full privileges.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Giving privileges to run the agent event viewer

The Symantec Critical System Protection agent includes the agent event viewer, which displays recent events that were reported by the agent.

As the administrator, you can allow all users, specific users, or specific user groups to run the agent event viewer. To do this, you must configure the agent event viewer options in the Windows prevention policies.

Allowing all users to run the agent event viewer

You can allow all users to run the agent event viewer.

To allow all users to run the agent event viewer

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 On the Policies page, in the Workspace tree, click the **Symantec** folder.

4 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

5 In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.

6 In the policy editor dialog box, under **Interactive Program Options > General Settings > SCSP Agent Tools**, check **Allow all users to run the SCSP agent event viewer**.

7 Click **OK** to save your changes.

8 Apply or reapply the policy to the agent.

Allowing specific users to run the agent event viewer

You can allow specific users to run the agent event viewer.

To allow specific users to run the agent event viewer

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.
6. In the policy editor dialog box, under **Interactive Program Options > General Settings > SCSP Agent Tools**, check **Allow specific users to run the SCSP agent event viewer**, and then click **Edit[+]**.
7. In the policy editor dialog box, under **List of users who can run SCSP agent event viewer**, click **Add**, and then add the users to the list of users allowed to run the agent event viewer.
8. Click **OK** to save your changes.
9. Apply or reapply the policy to the agent.

Allowing specific groups to run the agent event viewer

You can allow specific user groups to run the agent event viewer.

To allow specific groups to run the agent event viewer

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **Interactive Program Options**.
6. In the policy editor dialog box, under **Interactive Program Options > General Settings > SCSP Agent Tools**, check **Allow specific groups to run the SCSP agent event viewer**, and then click **Edit[+]**.
7. In the policy editor dialog box, under **List of groups that can run SCSP agent event viewer**, click **Add**, and then add the groups to the list of groups allowed to run the agent event viewer.

8 Click **OK** to save your changes.

9 Apply or reapply the policy to the agent.

Allowing granular access to files, devices, and registry keys

The following example globally blocks all access to File X, but allows User A and User B read access using Program App1 and Program App2,and User C and Group D write access using programs that are located in remote share path \\filesvr\trusted\.

To allow granular access to files, devices, and registry keys

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention**.

3 In the Workspace pane, select a Windows prevention policy, and then right-click **Edit Policy**.

4 In the policy editor dialog box, under **Policy Settings**, click **Process Sets**.

5 In the policy editor dialog box, under **Process Sets > Interactive Program Options > Specific Interactive Program Options**, click **Edit[+]** before **Default Interactive Program Options**.

6 Under **Default Interactive Program Options > File Rules > No-Access Resource Lists**, check **Block all access to these files**, click **Edit[+]** and then add File X.

7 Under **Default Interactive Program Options > File Rules > Read-only Resource Lists**, check **Block and log modifications to these files as trivial**, click **Edit[+]**and then add File X with program path *\app?.exe for User A.

8 Under **Default Interactive Program Options > File Rules > Read-only Resource Lists**, check **Block and log modifications to these files as trivial**, click **Edit[+]** and then add File X with program path *\app?.exe for User B.

9 Under **Default Interactive Program Options > File Rules > Writable Resource Lists**, check **Allow but log modifications to these files**, click **Edit[+]** and then add File X with program path \\filesvr\trusted\*.exe for User C.

10 Under **Default Interactive Program Options > File Rules > Writable Resource Lists**, check **Allow but log modifications to these files**, click **Edit[+]** and then add File X with program path \\filesvr\trusted\*.exe for Group D.

11 Click **OK** to save your changes.

12 Apply or reapply the policy to the agent.

Giving a program access to a specific resource set

Sometimes a program that requires access to a set of resources is denied access by the out-of-the-box prevention policies. While the prevention policies provide per-process resource control for default programs, you should create custom program options if there are more than a few resources or if more than one program requires the custom rules. Policy options let you assign a selected program to this custom options group, to define rules for it that do not apply to all the default programs. By doing this, you can allow programs assigned to the custom options group to access resources that are not accessible to other programs.

To give a program access to a specific resource set

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Workspace pane, select a prevention policy, and then right-click **Edit Policy**.
5. In the policy editor dialog box, under **Policy Settings**, click **My Custom Programs**.
6. In the policy editor dialog box, under **My Custom Programs**, click **Add a new Custom Control** icon.
7. In the **New Custom Control Wizard** dialog box, type a name and identifier for the custom program options, select **This program is interactive** category, and then click **Finish**.
8. In the policy editor dialog box, check the custom program that you have created, and then click **Edit[+]** before the custom program name.
9. Check **Specify interactive programs with custom privileges** and then click **Edit[+]** to add the custom interactive programs to the list.
10. (Optional) Adjust the remaining options.
11. Click **OK** to save the policy changes.
12. Apply or reapply the policy to the agent.

Giving a program wide access to resources

If a critical program generates policy violation events for many resources, and you want to allow the program access to all the denied resources, you may want to consider elevating the privilege level for this program. If the program already has a BCD, then you can change the privilege level for this program using the specific Alternate Privilege Options group.

For example, to give the DNS Server safe privileges, enable Policy Settings > Service Options > Core OS Service Options > DNS Server > Advanced Options > Alternate Privilege Level > Run with safe service privileges.

Sometimes a program does not have a specific BCD. An example for this scenario might be antivirus software that is not recognized by the out-of-the-box prevention policies. Policy options allow you to add security software to an already pre-defined host security process set. This is set using Policy Settings > Process Sets > Host Security Programs > Basic Options > Host security programs installed. Add the path to your security programs in a pre-populated list of other host security programs.

If the program does not have a BCD, and it is not a security program, you can give it safe or full privileges using the Alternate Privilege Level option, under the general group options. To give alternate privilege level to a service, enable Policy Settings > Service Options > Alternate Privilege Lists . To specify an interactive program with safe or full privilege, use Policy Settings > Interactive Program Options > Alternate Privilege Lists.

Allowing diagnostic programs to access process data

A policy option in the UNIX Protection policy allows diagnostic programs to access process data via the /proc file system.

To allow diagnostic programs to access process data

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, in the Workspace tree, click the **Symantec** folder.
4. In the Filters pane, click **Unix Policies**.
5. In the Workspace pane, select the Protection prevention policy, and then right-click **Edit Policy**.
6. In the policy editor dialog box, under **Policy Settings**, click **Process Sets**.
7. In the policy editor dialog box, under **Process Sets > Interactive Program Options > Specific Interactive Program Options** click **Edit[+]** before **Root Program Options [rootpriv_ps]**.
8. In the policy editor dialog box, under **General Settings > System Admin Otions**, check **Allow tools, such as truss and gcore, to access process data**.

9 Click **OK** to save the policy changes.

10 Apply or reapply the policy to the agent.

How to correctly block telnet, ftp, rlogin, and similar services

On UNIX operating systems, the inetd daemon handles the initial network connection of some services, such as telnet, ftp, and rlogin, before the services start. In the IPS policies, you can control the network connections for such services only by using the inetd pset. You cannot control the network connections from the service's own pset.

By default, the inbound network rules for the inetd pset allows connections to the following ports: ftp (21), lp (515), telnet (23), unix-rexec (512), unix-rlogin (513), unix-rsh (514), and tftp (69).

The network rules are applied in the following order:

- Pset-specific rules
- Group level (daemon or interactive) rules
- Global rules

For example, if you have an Allow rule for telnet(23) in the inetd pset inbound network rules, any group level or global network rules that you add to restrict telnet will have no effect.

Appendix A

Parameter reference syntax

This appendix includes the following topics:

- Parameter reference syntax overview
- Simple policy parameter
- Compound policy parameter
- Operating system environment variable
- Windows registry value
- Agent translator function

Parameter reference syntax overview

Table A-1 lists the types of references that Symantec Critical System Protection supports in parameter values. These can be references to parameters defined elsewhere in the policy or data on the operating system.

Table A-1 Types of references with syntax

Type	Syntax
Simple policy parameter	%parameter%
Compound policy parameter	%parameter:field%
OS Environment variable	%environmentvariable%
Windows Registry value	%%registrypath%%
Agent Translator Function	%?function(parameters)?%

Inside the reference delimiters, you must escape any special characters that are used in strings by using a forward slash (/) on Windows and a backslash (\) on UNIX.

Note: The syntax is the same for policy parameters and OS environment variables. The Symantec Critical System Protection agent looks for a policy parameter with the given name first. If the policy parameter is not found, it looks for an OS environment variable.

See “Simple policy parameter” on page 110.

See “Compound policy parameter” on page 110.

See “Operating system environment variable” on page 114.

See “Windows registry value” on page 114.

See “Agent translator function” on page 115.

Simple policy parameter

A simple parameter is a list of single values. You reference the parameter by its name – no field names are necessary since a simple parameter is a list of single values. The agent replaces the parameter reference with the values. Parameter names are case sensitive.

The simple policy parameter types are mentioned as follows:

String	A single string value.
String List	A list of string values.
Date/Time Duration	A single duration value, e.g 30 minutes.
Date/Time Interval	A single repetition interval, e.g. hourly, daily.

See “Parameter reference syntax overview” on page 109.

Compound policy parameter

A compound policy parameter is a list of sets of values. In the console, a compound parameter is displayed as a table, where each row is one parameter value and the columns are the fields in the value. For each compound parameter type, there is a specific set of fields in the list. When referencing a compound parameter, you must use the parameter name followed by a colon and a field name. You must always refer to a specific field. For example, you might use **%myparameter:prog%**. Parameter and field names are case sensitive.

The compound policy parameter types along with their field names are mentioned as follows:

Compound policy parameter	Description
Process List	A list of processes, each element in the list consisting of one or more process attributes. See "Process List" on page 111.
Process List without Arguments	A list of processes, each element in the list consisting of one or more process attributes that excludes the command line arguments attribute. See "Process List without Arguments" on page 112.
Resource List	A list of resources such as file paths and registry paths, where each element consists of a resource name and zero or more process attributes. See "Resource List" on page 112.
Network List with Processes	A list of network rules, where each element consists of network connection attributes, process attributes, and action attributes. See "Network List with Processes" on page 113.
Network List	A list of network rules, where each element consists of network connection attributes and action attributes. See "Network List" on page 113.
Date/Time Value	A single date/time value with a timezone. See "Date/Time Value" on page 114.

See "Parameter reference syntax overview" on page 109.

Process List

Process List is a list of processes, where each element in the list consists of one or more process attributes.

- The **prog** field is the **Program Path** column and is required in each row. It specifies the program running in the process.
- The **cmdline** field is the **Arguments** column, specifying the command line parameters for the process. This field is optional.

- The **id** field is the **User Name** column, specifying the username for the process. This field is optional.
- The **groupid** field is the **User Name** column, specifying the group name for the process. This field is optional.

Note: If you want to specify all processes for a specific user, you must still fill in the **Program Path** column, but you can use a ***** to specify all programs and then fill in the **User Name** column to specify the desired user account.

Process List without Arguments

Process List without Arguments is a list of processes, where each element in the list consists of one or more process attributes that excludes the command line arguments attribute.

- The column and field names are identical to the Process List parameter type except the **Arguments** field is not included.

Resource List

Resource List is a list of resources such as file paths, registry paths, and process paths), where each element consists of a resource name and zero or more process attributes.

- The **value** field is the **Resource Path** column and is required in each row. It specifies the file or registry path you are controlling.
- The **prog** field is the **Program Path** column. This field is required if you want to specify other process attributes. Otherwise it is optional.
- The **cmdline** field is the **Arguments** column, specifying the command line parameters for the process. This field is optional.
- The **id** field is the **User Name** column, specifying the username for the process. This field is optional.
- The **groupid** field is the **User Name** column, specifying the group name for the process. This field is optional.

Note: If you want to specify all processes for a specific user, you must still fill in the **Program Path** column, but you can use a ***** to specify all programs and then fill in the User Name column to specify the desired user account.

Network List with Processes

Network List with Processes is a list of network rules, where each element consists of network connection attributes, process attributes, and action attributes.

- Connection information:
  - The **protocol** field is the **Protocol** column.
  - One or more additional connection elements are required:
    - **RPort** field is the **Remote Port** column and specifies the remote port or port range.
    - **LPort** field is the **Local Port** column and specifies the local port or port range.
    - **RIP** field is the **Remote IP** column and specifies the remote IP address or address range.
- Action information:
  - The **action** field is the **Action** column.
  - The **log** field is the **Logging** column.
- Process information:
  - The **prog** field is the **Program Path** column. This field is required if you want to specify other process attributes. Otherwise it is optional.
  - The **cmdline** field is the **Arguments** column, specifying the command line parameters for the process. This field is optional.
  - The **id** field is the **User Name** column, specifying the username for that process. This field is optional.
  - The **groupid** field is the **User Name** column, specifying the group name for the process. This field is optional.

Note: If you want to specify all processes for a specific user, you must still fill in the **Program Path** column, but you can use a `*` to specify all programs and then fill in the User Name column to specify the desired user account.

Network List

Network List is a list of network rules, where each element consists of network connection attributes and action attributes.

- The column and field names are identical to the Network Process List parameter type, except the process-related fields are not included.

Date/Time Value

Date/Time Value is a single date/time value with a timezone.

- This compound parameter type is not displayed as a table because it cannot be a list.
- The field name for the **Date** and **Timezone** fields in the Console are **value** and **timezone**, respectively.

Operating system environment variable

You can use an operating system environment variable as a variable in a policy. Environment variable names follow the operating system's normal conventions for case sensitivity, so they are case sensitive on UNIX and case insensitive on Windows.

Note: The environment variables are evaluated in the context of the SCSP agent IPS Service or daemon. Therefore, you should only reference the environment variables that have system-wide values. If you reference a variable with a user-specific value, you get the value for the IPS Service or daemon user, which is probably not the desired value.

See "Parameter reference syntax overview" on page 109.

Windows registry value

For registry references, the agent looks up the given value in the registry and replaces the reference with the data that the value contains.

The data must be one of the following types:

- REG_SZ (string)
- REG_EXPAND_SZ (string with environment variables that should be expanded)
- REG_MULTI_SZ (list of strings)
- REG_DWORD (32-bit integer)
- REG_QWORD (64-bit integer)

The agent expands an environment variable's REG_EXPAND_SZ values immediately, before it processes the resulting string. For REG_MULTI_SZ values, the reference expands to the list of strings.

On 64-bit versions of Windows, you can prefix registry paths with an optional redirection specification. This redirection specification specifies how registry redirection should be used when looking up the path.

The valid redirection specifications are as follows:

- 32: redirection is turned off or on to give a 32-bit program's view of the registry
- 64: redirection is turned off or on to give a 64-bit program's view of the registry
- 6432: looks in the 64-bit view of the registry first, and then if that fails, looks in the 32-bit view
- 3264: looks in the 32-bit view of the registry first, and then if that fails, looks in the 64-bit view

See "Parameter reference syntax overview" on page 109.

Agent translator function

A function reference provides a way to call an extension function from within a policy. The agent replaces the function reference with the return value or list of return values of the function.

In a function reference such as `%?function(parameters)?%`, the parameters may contain any characters, even special characters, except that you must escape a close parenthesis ")" . The function parameters are not processed, so if they contain a reference themselves, the text of the reference is passed to the function. For example, `%myvar%` is passed rather than myvar's value after evaluation. However, if a function's return value contains a reference, the reference is subsequently evaluated.

See "*Translator function reference*" on page 117.

Appendix B

Translator function reference

This appendix includes the following topics:

Generic functions

The following functions can be used in both Prevention and Detection policies and can be used on all operating systems:

- %?LocalIPs()?%
  See “%?LocalIPs()?%” on page 117.
- %?LocalIPAddresses()?%
  See “%?LocalIPAddresses()?%” on page 118.
- %?AgentParams(<param name>)?%
  See “%?AgentParams(<param name>)?%” on page 118.
- %?SplitPath(<path>)?%
  See “%?SplitPath(<path>)?%” on page 118.
- %?ImportFileList(<filepath>)?%
  See “%?ImportFileList(<filepath>)?%” on page 118.

%?LocalIPs()?%

Returns the list of IP addresses for the system. Includes only IPv4 addresses.

%?LocalIPAddresses()?%

Returns the list of IP addresses for the system. Includes both IPv4 and IPv6 addresses.

%?AgentParams(<param name>)?%

Looks in the IPS agent.ini file and returns the requested parameter. The following strings are valid as "param name":

- Notification Port: returns the port the agent listens on for notifications
- Server IP: returns the list of IP addresses for management servers this agent can connect to
- Server Port: returns the management server port this agent connects to

For example: %?AgentParams(Notification Port)?%

%?SplitPath(<path>)?%

Takes a pathname and puts out a list consisting of the original pathname plus all the directory names on the pathname leading up to it.

For example, if you call %?SplitPath(C:\a\b\c)?% you get:

- C:\a
- C:\a\b
- C:\a\b\c

%?ImportFileList(<filepath>)?%

Takes a filepath and imports the data from the file into the policy as if a user had typed that data into the console. This data can be filepaths, registry keys, usernames, groupnames or any other strings that make sense at the point in the policy where the function is called.

By default, the file being imported is limited to 100 lines. This limit is defined in the ips.importfile.maxlines setting in the IPS/agent.ini file and can be adjusted if larger files are required.

Note: This function can be made optional by using in the following way : %?-ImportFileList(<path>)?% In this case, the translator will translate successfully even if the file to be imported is not available.

Note: To make the data inside the file to be optional, add a "-" in front of each optional line. For example, if the file you want to import has usernames in the file and certain user names are to be made optional then the file data should be:

admin

test1

-test2 (For an optional user)

Prevention policy functions

The following functions can only be used in Prevention policies. Some functions are supported on all operating systems that support Prevention. Other functions are supported only on certain operating systems.

See “Functions for all prevention operating systems” on page 119.

See “Functions for Windows only” on page 120.

See “Function for *nix operating sytems that support prevention” on page 122.

Functions for all prevention operating systems

Following are the functions used for prevention in all operating systems:

- %?LocalSubnets()?%
  See “%?LocalSubnets()?%” on page 119.
- %?LocalSubnetsIPv4()?%
  See “%?LocalSubnetsIPv4()?%” on page 120.

See “Prevention policy functions” on page 119.

%?LocalSubnets()?%

Returns the list of all local IP addresses(both IPv4 and IPv6) with their subnets for the system. The formats are as follows:

- IPv4 Address: xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx
- IPv6 Address: xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/xx (for Linux and AIX)
- xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx (Solaris)

%?LocalSubnetsIPv4()?%

Returns the list of all local IPv4 addresses with their subnets for the system. The formats are as follows:

- IPv4 Address: xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx

Functions for Windows only

Following are the functions used for prevention in Windows operating systems:

- %?SIDToName(<windows SID>)?%
  See "%?SIDToName(<windows SID>)?%" on page 120.
- %?XMLAttrValueList(XML_file_path,element_name_to_match,attr_name_to_match,flags)?%
  See "%?XMLAttrValueList(XML_file_path,element_name_to_match,attr_name_to_match,flags)?%" on page 120.
- %?OsVersionMatch(<major.minor>,<message>)?%
  See "%?OsVersionMatch(<major.minor>,<message>)?%" on page 121.
- %?VirtualRoot(<virtual root reg key>)?%
  See "%?VirtualRoot(<virtual root reg key>)?%" on page 121.
- %?RegValueList(registry_path,string_to_exclude,prefix,suffix)?%
  See "%?RegValueList(registry_path,string_to_exclude,prefix,suffix)?%" on page 121.

%?SIDToName(<windows SID>)?%

Translates the SID into the account or group name. Typically used with well-known SIDs.

For example:

%?SIDToName(S-1-5-32-544)?%

This translates the SID specified to the built-in "Administrators" group name.

%?XMLAttrValueList(XML_file_path,element_name_to_match,attr_name_to_match,flags)?%

The function finds the file at "XML_file_path", looks in it for the "attr_name_to_match" in the "element_name_to_match" and returns the value(s) of the attr, if found.

The "flags" argument is optional and determines whether to look in the 32-bit view of the filesystem or the 64-bit view (they differ due to WOW64 file redirection in Win64). The flags can be blank, "32", "64", "3264," or "6432." A blank flag or

"32" means use the 32-bit view, "64" means use the 64-bit view, and "3264" or "6432" means to try both, using the order given.

For example:

%?XMLAttrValueList(%systemroot%\system32\inetsrv\Metabase.xml, IIsWebVirtualDir,Path)?%

This returns the value of the Path attribute within the IIsWebVirtualDir element in the Metabase.xml XML file, if the attribute is found.

%?OsVersionMatch(<major.minor>,<message>)?%

Checks whether the agent OS matches the major/minor combination passed in. If the OS matches, throw a fatal translation error, using the "message" supplied. This is used to prevent version-specific policies from being used on the wrong version of an OS.

For example:

%?OsVersionMatch(4.0,"This IPS policy cannot be applied to Windows NT!")?%

This does not allow the IPS policy in which the function is used to be applied to Windows NT OS and throw the translator error on the management console.

%?VirtualRoot(<virtual root reg key>)?%

Reads the registry structure under the IIS "Virtual Root" key and returns the list of virtual web site folders. This function is very specialized for a specific IIS registry value and probably not useful for other purposes.

For example:

%?VirtualRoot(HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots)?%

%?RegValueList(registry_path,string_to_exclude,prefix,suffix)?%

Look in the "registry_path" and return the list of values found there.

- If "string_to_exclude" is passed in, exclude that string from the returned value list.
- If "prefix" is passed in, prepend that prefix string to every value returned.
- If "suffix" is passed in, append that suffix string to every value returned.

The registry_path argument is required, all the others are optional (they can be blank or omitted completely).

This function is very specialized for the MS SQL Server registry structure and probably not useful for other purposes.

For example:

%?RegValueList(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\
InstalledInstances,MSSQLSERVER,%%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Microsoft SQL Server\,\Setup\SQLPath%%\binn\sqlservr.exe)?%

This excludes the MSSQLSERVER string from the returned value list. It also prepends the prefix and appends the suffix string to each value returned.

Function for *nix operating sytems that support prevention

%?UtilParams(<param name>)?%

Looks in the IPS util.ini file and returns the requested parameter. The following strings are valid as parameters:

- Service Port: returns the port the Util daemon on this agent listens on

For example

%?UtilParams(Service Port)?%