Symantec™ Critical System Protection Version 5.2 RU8 Windows Baseline 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: 5.2.8

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Bloodhound, Confidence Online, Digital Immune System, LiveUpdate, Norton, Sygate, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "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 maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/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

Introducing the Windows Baseline policy

This chapter includes the following topics:

Introduction

The Symantec Critical System Protection Host Intrusion Detection policies have been redesigned and rewritten. Multiple policies were reorganized into a baseline monitoring solution for the Windows operating system environment. The new policy provides enhanced stability, greater ease of use and detection accuracy, and added functionality.

The Windows policy includes the following improvements:

- The IDS policy was rewritten to improve functionality and accuracy in monitoring security events.
- The file monitoring area was redesigned and rewritten to provide a large number of new file and directory monitoring functions. For example, you can control and enable the access, delete, modify, and create change monitoring functions by group.
- You can perform advanced rule-by-rule tuning directly from the Symantec Critical System Protection console. These rules also use ignore logic and select logic methodology.

- You can configure and view all rule content from the Symantec Critical System Protection console, which removes the need to use the Authoring Tool.
- Policy option group naming conventions have been standardized for ease of administration. You can enable and disable entire areas of the policies with option check boxes.
- Automatic application detection has been updated to enable and disable monitoring without the need for administrators to configure the policy individually per host.
- You can configure many parameter options individually for each rule. For example, you can configure the Rule Name, Rule Severity, and Rule monitoring content separately for each rule.
- You can select a severity level for each rule. You no longer need to know specific numerical values for the severity base types.
- New Web attack detection functionality has been built into the policy to provide monitoring of Web attacks. The types of attacks that are detected include basic SQL injection, directory transversal, vulnerable CGI requests, blacklist IP functionality, and vulnerability scanning detection. Malicious request strings, malicious extension requests, and malicious user agent strings are also detected.
- You can mouse over parts of the user interface to display descriptions to assist in policy navigation and rule-by-rule overview.

Table 1-1 illustrates how the existing policies from previous releases were combined with new options into the 5.2.6 top level option groups.

Table 1-1 Detection options organization map

Options in previous releases, with new material noted	Detection option organization in release 5.2.6
System_Group_Management_Change System_User_Configuration Enhanced_System_Group_Change (NEW)	System User and Group Change Monitor
Domain_Trust_Configuration MS_ActiveDirectory_FSMO_Changed System_AuthEncrypt_Configuration AD_Priviledged_Group/User_Change (NEW)	System Active-Directory Change Monitor

Table 1-1 Detection options organization map *(continued)*

Options in previous releases, with new material noted	Detection option organization in release 5.2.6
System_Logoff System_Logon_Success System_Failed_Access_Status Domain_Priviledged_User_Login (NEW)	System Login Activity and Access Monitor
System_Autorun_Configuration Network_Comm_Configuration System_File_Protection_Status System_Security_Configuration System_StartStop_Options System_Audit_Tampering System_ Hardening	System Hardening Monitor
System_Shares_ Configuration Host_IDS_File_Tampering Critical_System_File_Monitor (NEW)	System File and Directory Monitor
Critical_ Registry_StartPath_Monitor Critical_ System_Registry_Monitor (NEW)	System Registry Monitor
Symantec_AV_Client_Communication SAV_Critical_Action_Monitor (NEW) SEP_Critical_Action_Monitor (NEW)	Symantec Software Monitoring
USB_Device_Activity USB_Device_Vendor_Detection (NEW) CD/DVD_Burning_Activity (NEW)	External Device Activity Monitor
Generic_Web_Attack_Detection Web_Attack_Detection (NEW)	System Attack Detection

File monitoring improvements

Specific file monitoring changes include the following improvements:

- You can control and enable the access, delete, modify, and create change monitoring functions on a group-by-group basis.
- You can control modification diff'ing, including algorithm selection on a group-by-group basis.
- You can set date and time restrictions within each specific file monitoring group.
- You can tune the file monitor modified detection operation for specific criteria, such as only for permission changes, size changes, bitmask changes, and so on.
- You can use specific ignore logic criteria and select logic criteria in each file monitoring group. For example, you can independently configure each file monitoring group to ignore file paths or strings.

Windows-specific policy improvements

Windows-specific policy changes include the following improvements:

- Product-specific monitoring areas for key Symantec applications such as Symantec AntiVirus and Symantec Endpoint Protection. Improved monitoring of endpoint security products provides administrators more finite events that are tailored for compatibility.
- Improved external device detection now includes event generation for CD and DVD burning activity.
- Critical Windows registry change detection has been added. Critical auto start areas of the Windows operating system are monitored to ensure that the host system security is maintained. New registry paths for Auto Start Keys have been added.

Note: Registry monitoring has the same options as the rewritten file and directory monitoring.

Console changes

Symantec Critical System Protection provides specific content control per rule from the console. Each rule in the Baseline policy has required parameters. These rules are now viewable and customizable from the console.

The options in Table 1-2 are available for each rule that is displayed in the **Policy Settings** pane.

Table 1-2 Rule options

Option	Description
Rule Name	The name that is associated with the rule that generates the specific event. A single string value is allowed in the string field.
Severity	The severity of event. Available for each rule of the policy. You can only select one severity level, Info, Notice, Warning, Major, or Critical, for each rule.
Event IDs	Parameter options for Windows event log watch rules. Separate multiple event IDs with a comma (,) in this string list. You can add, edit, and remove event IDs.
File Paths	Parameter options for file watch rules. You can use multiple file paths with associated wildcard entries in this string list. You can add, edit, and remove file paths.
Registry Paths	Parameter options for registry watch rules. You can use multiple Windows registry paths with associated wildcard entries in this string list. You can add, edit, and remove registry paths.
Select Strings	Used in rule select logic. Symantec Critical System Protection uses primary logic or initial sifting method for rule event generation. Use an asterisk (*) to select all the events that the criteria that you entered previously generate. For example, criteria such as (event IDs, file paths, registry paths, or log strings previously defined. With this option you can specifically tune rules for administrator needs. For example, if you change the select string on a file watch rule from * to *Permission*, then that rule only generates a file watch event if that event contains the string “Permission.” You can have multiple select strings in this string list. All strings are case insensitive. You can add, edit, and remove select strings.
Ignore Strings	Used in rule ignore logic. Symantec Critical System Protection uses secondary ignore logic or ignore sifting method for rule event generation. Almost all rule parameter options contain a blank value, which signifies that a null value or no value is associated with the ignore logic statement. Symantec Critical System Protection ignores any string in this field other than blank value upon pattern matching on the final event generation. Ignore strings also provide you with the ability to perform advanced rule-by-rule tuning. You can have multiple ignore strings in this string list. All strings are case insensitive. You can add, edit, and remove ignore strings.

Note: Each parameter is preconfigured with default values to ensure the functionality of the rule. Changes to rule name and severity do not affect the overall operation of the rule.

Chapter 2

Policy options

This chapter includes the following topics:

System User and Group Change Monitor

This option group section of the policy monitors for specific user and group change-based events.

System User Configuration Changes

This option group subsection monitors user changes from local account manipulation to the user activity that warrants event detection in Active Directory environments.

Table 2-1 Description of the **Account Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Account Changed
Rule Name	ZZ_Account_Changed
Severity	Warning
Event IDs	642, 4738, 685
Description	Detects the changes that are made to user accounts on the local system.

Table 2-2 Description of the **Account Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Account Created
Rule Name	AA_Account_Created
Severity	Warning
Event IDs	629, 4725
Description	Detects the creation of user accounts on the local system.

Table 2-3 Description of the **Account Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Account Deleted
Rule Name	Account_Deleted
Severity	Warning
Event IDs	630, 4720
Description	Detects the deletion of user accounts on the local system.

Table 2-4 Description of the **Account Disabled** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Account Disabled
Rule Name	Account_Disabled
Severity	Warning
Event IDs	629, 4725
Description	Detects the disabling of user accounts on the local system.

Table 2-5 Description of the **Account Enabled** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Account Enabled
Rule Name	Account_Enabled
Severity	Warning
Event IDs	626, 4722
Description	Detects the enabling of user accounts on the local system.

Table 2-6 Description of the **Local Account Lock Out Threshold, Time Interval, and Severity** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Local Account Lock Out Threshold, Time Interval, and Severity
Rule Name	Local_Account_Locked_Out_After_*user defined*_Tries
Severity	Critical
Event IDs	644,4750
Count	10

Table 2-6 Description of the **Local Account Lock Out Threshold, Time Interval, and Severity** parameters used *(continued)*

Parameter	Description
Interval	3
Description	Detects the locking of a user account on the local system then generates a higher severity event based on user-defined threshold values.

Table 2-7 Description of the **Local Account Locked Out** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Local Account Locked Out
Rule Name	Local_Account_Locked_Out
Severity	Warning
Event IDs	644, 4750
Description	Detects the locking of a user account on the local system.

Table 2-8 Description of the **Local Account Unlocked** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Local Account Unlocked
Rule Name	Local_Account_Unlocked
Severity	Warning
Event IDs	671, 4767
Description	Detects the unlocking of a user account on the local system.

Table 2-9 Description of the **Admin Passwd Change Failed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Admin Passwd Change Failed
Rule Name	Admin_Passwd_Change_Failed
Severity	Critical
Event IDs	627, 4723
Description	Detects the failed attempts to change the administrator password.

Table 2-10 Description of the **User Added to Global Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Added to Global Group
Rule Name	User_Added_to_Global_Group
Severity	Warning
Event IDs	632, 4728
Description	Detects the addition of a user to a global group. This rule applies to Windows servers that act as domain controllers.

Table 2-11 Description of the **User Removed from Global Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Removed from Global Group
Rule Name	User_Removed_from_Global_Group
Severity	Warning
Event IDs	633, 4729

Table 2-11 Description of the **User Removed from Global Group** parameters used *(continued)*

Parameter	Description
Description	Detects the addition of a user to a global group. This rule applies to Windows servers that act as domain controllers.

Table 2-12 Description of the **Guest Password Change Failed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Guest Password Change Failed
Rule Name	Guest_Passwd_Change_Failed
Severity	Critical
Event IDs	627, 4723
Description	Detects a failed attempt to change the guest's password.

Table 2-13 Description of the **User Added to Local Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Added to Local Group
Rule Name	User_Added_to_Local_Group
Severity	Warning
Event IDs	636, 4732
Description	Detects the addition of a user to a local group.

Table 2-14 Description of the **User Removed from Global Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes

Table 2-14 Description of the **User Removed from Global Group** parameters used *(continued)*

Parameter	Description
Option	User Removed from Global Group
Rule Name	User_Removed_from_Global_Group
Severity	Warning
Event IDs	637, 4733
Description	Detects the removal of a user from a global group. This rule applies to the Windows servers that act as domain controllers.

Table 2-15 Description of the **Right Assigned** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Right Assigned
Rule Name	Right_Assigned
Severity	Warning
Event IDs	608, 4704, 4717
Description	Detects that an access right has been assigned to a user.

Table 2-16 Description of the **Right Removed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Right Removed
Rule Name	Right_Removed
Severity	Warning
Event IDs	609, 4705, 4718
Description	Detects that an access right has been removed from a user.

Table 2-17 Description of the **User Password Change Failed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Password Change Failed
Rule Name	User_Password_Change_Failed
Severity	Warning
Event IDs	627, 4723
Description	Detects the failed attempt to change a user's password.

Table 2-18 Description of the **User Added to Universal Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Added to Universal Group
Rule Name	User_Added_to_Universal_Group
Severity	Warning
Event IDs	660, 4756
Description	Detects the addition of a user to a universal group. This rule applies to the Windows servers that act as domain controllers.

Table 2-19 Description of the **User Removed from Universal Grp** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Removed from to Universal Grp
Rule Name	User_Removed_from_Universal_Grp
Severity	Warning
Event IDs	661, 4757

Table 2-19 Description of the **User Removed from Universal Grp** parameters used *(continued)*

Parameter	Description
Description	Detects the removal of a user from a universal group. This rule applies to the Windows servers that act as domain controllers.

Table 2-20 Description of the **User Added to Local Distribution Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Added to Local Distribution Group
Rule Name	User_Add_Local_Distribution_Grp
Severity	Warning
Event IDs	650, 4746
Description	Detects the addition of a user to a local distribution group.

Table 2-21 Description of the **User Added to Global Distribution Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Added to Global Distribution Group
Rule Name	User_Add_Global _Distribution_Grp
Severity	Warning
Event IDs	655, 4751
Description	Detects the addition of a user to a global distribution group.

Table 2-22 Description of the **User Added to Universal Distribution Group** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Added to Universal Distribution Group
Rule Name	User_Add_Univ_Distribution_Grp
Severity	Warning
Event IDs	665, 4761
Description	Detects the addition of a user to a universal distribution group.

Table 2-23 Description of the **Administrator Changed Admin Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Administrator Changed Admin Password
Rule Name	Admin_Changed_Admin_Passwd
Severity	Warning
Event IDs	627, 628, 4723, 4724
Description	Detects that the administrator changed the administrator's own password.

Table 2-24 Description of the **Guest Changed Admin Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Guest Changed Admin Password
Rule Name	Guest_Changed_Admin_Passwd
Severity	Critical

Table 2-24 Description of the **Guest Changed Admin Password** parameters used *(continued)*

Parameter	Description
Event IDs	627, 628, 4723, 4724
Description	Detects that a guest changed the administrator password.

Table 2-25 Description of the **User Changed Admin Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Changed Admin Password
Rule Name	User_Changed_Admin_Passwd
Severity	Major
Event IDs	627, 628, 4723, 4724
Description	Detects that a user changed the administrator password.

Table 2-26 Description of the **Administrator Changed Guest Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Administrator Changed Guest Password
Rule Name	Admin_Changed_Guest_Passwd
Severity	Warning
Event IDs	627, 628, 4723, 4724
Description	Detects that the administrator changed the guest password.

Table 2-27 Description of the **Guest Changed Guest Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Guest Changed Guest Password
Rule Name	Guest_Changed_Guest_Passwd
Severity	Notice
Event IDs	627, 628, 4723, 4724
Description	Detects that the guest changed the guest password.

Table 2-28 Description of the **User Changed Guest Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Changed Guest Password
Rule Name	User_Changed_Guest_Passwd
Severity	Notice
Event IDs	627, 628, 4723, 4724
Description	Detects that a user changed the guest password.

Table 2-29 Description of the **Administrator Changed User Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Administrator Changed User Password
Rule Name	Admin_Changed_User_Passwd
Severity	Notice
Event IDs	627, 628, 4723, 4724

Table 2-29 Description of the **Administrator Changed User Password** parameters used *(continued)*

Parameter	Description
Description	Detects that the administrator changed a user's password.

Table 2-30 Description of the **Guest Changed User Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Guest Changed User Password
Rule Name	Guest_Changed_User_Passwd
Severity	Warning
Event IDs	627, 628, 4723, 4724
Description	Detects that the guest changed the user's password.

Table 2-31 Description of the **User Changed User Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Changed User Password
Rule Name	User_Changed_User_Passwd
Severity	Notice
Event IDs	627, 628, 4723, 4724
Description	Detects that the user changed another user's password.

Table 2-32 Description of the **Administrator Changed Guest Password** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	Administrator Changed Guest Password

Table 2-32 Description of the **Administrator Changed Guest Password** parameters used *(continued)*

Parameter	Description
Rule Name	Admin_Changed_Guest_Passwd
Severity	Notice
Event IDs	627, 628, 4723, 4724
Description	Detects that the administrator changed the guest password.

System Group Changes

This option group subsection detects group changes by monitoring the manipulation of the following groups:

- Global groups
- Local groups
- Universal groups
- Local distribution groups
- Global distribution groups
- Universal distribution groups

It monitors the security-relevant changes that warrant event detection.

Event detection includes administrator actions such as creation, change, or deletion of security-enabled local, global, or universal groups. Security groups allow the system administrator or domain administrator to establish a standard set of user permissions for application groups of users. Changes, additions, or deletions to the security groups are normal behavior in an extended enterprise if the system administrator actively manipulates these groups. If the system administrator or domain administrator does not actively manipulate security groups, these events can indicate illegitimate activity.

Table 2-33 Description of the **Global Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Global Group Changed
Rule Name	Global_Group_Changed

Table 2-33 Description of the **Global Group Changed** parameters used *(continued)*

Parameter	Description
Severity	Info
Event IDs	641, 4737
Description	Detects that a global group was changed.

Table 2-34 Description of the **Global Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Global Group Created
Rule Name	Global_Group_Created
Severity	Warning
Event IDs	631, 4727
Description	Detects that a global group was created.

Table 2-35 Description of the **Global Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Global Group Deleted
Rule Name	Global_Group_Deleted
Severity	Warning
Event IDs	634, 4730
Description	Detects that a global group was deleted.

Table 2-36 Description of the **Local Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Local Group Changed

Table 2-36 Description of the **Local Group Changed** parameters used *(continued)*

Parameter	Description
Rule Name	Local_Group_Changed
Severity	Info
Event IDs	639, 4735
Description	Detects that a local group was changed.

Table 2-37 Description of the **Local Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Local Group Created
Rule Name	Local_Group_Created
Severity	Warning
Event IDs	635, 4731
Description	Detects that a local group was created.

Table 2-38 Description of the **Local Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Local Group Deleted
Rule Name	Local_Group_Deleted
Severity	Warning
Event IDs	638, 4734
Description	Detects that a local group was deleted.

Table 2-39 Description of the **Universal Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes

Table 2-39 Description of the **Universal Group Changed** parameters used *(continued)*

Parameter	Description
Option	Universal Group Changed
Rule Name	Universal_Group_Changed
Severity	Info
Event IDs	659, 4755
Description	Detects that a universal group was changed.

Table 2-40 Description of the **Universal Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Universal Group Created
Rule Name	Universal_Group_Created
Severity	Warning
Event IDs	658 4754
Description	Detects that a universal group was created.

Table 2-41 Description of the **Universal Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Universal Group Deleted
Rule Name	Universal_Group_Deleted
Severity	Warning
Event IDs	662, 4758
Description	Detects that a universal group was deleted.

Table 2-42 Description of the **Local Distribution Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Local Distribution Group Created
Rule Name	Local_Distribution_Grp_Created
Severity	Warning
Event IDs	648, 4744
Description	Detects when a local distribution group was created. The distribution lists can be created and managed through Active Directory MMC. Local distribution groups can include other groups and accounts from Windows Server 2003, Windows 2000, or Windows NT domains, and can be granted permissions only within a domain.

Table 2-43 Description of the **Local Distribution Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Local Distribution Group Changed
Rule Name	Local_Distribution_Grp_Changed
Severity	Warning
Event IDs	649, 4745
Description	Detects when a local distribution group was changed.

Table 2-44 Description of the **Local Distribution Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Local Distribution Group Deleted
Rule Name	Local_Distribution_Grp_Delete
Severity	Warning

Table 2-44 Description of the **Local Distribution Group Deleted** parameters used *(continued)*

Parameter	Description
Event IDs	652, 4748
Description	Detects when a local distribution group was deleted.

Table 2-45 Description of the **Global Distribution Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Global Distribution Group Created
Rule Name	Global_Distribution_Grp_Created
Severity	Warning
Event IDs	653, 4749
Description	Detects when a global distribution group was created. The distribution lists can be created and managed through Active Directory MMC. Local distribution groups can include other groups and accounts only from the domain in which the group is defined. They can be granted permissions in any domain in the forest.

Table 2-46 Description of the **Global Distribution Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Global Distribution Group Changed
Rule Name	Global_Distribution_Grp_Changed
Severity	Warning
Event IDs	654, 4750
Description	Detects when a global distribution group was changed.

Table 2-47 Description of the **Global Distribution Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Global Distribution Group Deleted
Rule Name	Global_Distribution_Grp_Deleted
Severity	Warning
Event IDs	657, 4753
Description	Detects when a global distribution group was deleted.

Table 2-48 Description of the **Universal Distribution Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Universal Distribution Group Created
Rule Name	Univ_Distribution_Grp_Created
Severity	Warning
Event IDs	663, 4759
Description	Detects when a universal distribution group was created. The distribution lists can be created and managed through Active Directory MMC. Universal distribution groups can include other groups and accounts from any domain in the domain tree or forest. They can be granted permissions in any domain in the domain tree or forest.

Table 2-49 Description of the **Universal Distribution Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Universal Distribution Group Changed
Rule Name	Univ_Distribution_Grp_Changed
Severity	Warning

Table 2-49 Description of the **Universal Distribution Group Changed** parameters used *(continued)*

Parameter	Description
Event IDs	664, 4760
Description	Detects when a universal distribution group was changed.

Table 2-50 Description of the **Universal Distribution Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Changes
Option	Universal Distribution Group Deleted
Rule Name	Univ_Distribution_Grp_Deleted
Severity	Warning
Event IDs	667, 4763
Description	Detects when a universal distribution group was deleted.

System Active Directory Change Monitor

This option group section of the policy monitors specific Active Directory-based events. These events include potentially suspicious domain trust events, FSMO changes, and authentication or encryption configuration changes. These events may be indicative of malicious configuration, which may affect the Active Directory system itself, as well as downstream systems.

Active Directory Domain Trust Configuration

This portion of the policy detects the creation or removal of a trusted domain relationship and changes to the Windows Domain Policy. Domain Trust relationships allow multiple Windows domains to share resources. They also allow users from one domain to log on and interact as trusted users in a foreign domain. Creation or removal of trusted domain relationships is expected behavior in extended enterprises. If this behavior is unexpected, it could indicate a serious security compromise at the domain level. Configuration: Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Audit Policy > Audit account management for success and failure, Audit policy change for success or failure.

Table 2-51 Description of the **Trust Domain Created** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory Domain Trust Configuration
Option	Trust Domain Created
Rule Name	Trust_Domain_Created
Severity	Warning
Event IDs	610, 4706
Description	Detects the creation of a trusted domain relationship with the primary domain controller.

Table 2-52 Description of the **Domain Policy Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory Domain Trust Configuration
Option	Domain Policy Changed
Rule Name	Domain_Policy_Changed
Severity	Warning
Event IDs	643, 4739
Description	Detects all Windows Domain Policy changes.

Table 2-53 Description of the **Trusted Domain Created** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory Domain Trust Configuration
Option	Trusted Domain Changed
Rule Name	Trusted_Domain_Changed
Severity	Warning
Event IDs	620, 4716
Description	Detects the modification of the trusted domain information.

Table 2-54 Description of the **Trusted Domain Removed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory Domain Trust Configuration
Option	Trusted Domain Removed
Rule Name	Trusted_Domain_Removed
Severity	Warning
Event IDs	611, 4707
Description	Detects the removal of a trusted domain relationship from the primary domain controller.

Active Directory FSMO Changes

This option group sub-section monitors changes to Active Directory's Flexible Single Master of Operation (FISMO). Changes to Schema Master, Domain Master, RID Master, PDCEmulator, and Infrastructure Master are critical functions of Active Directory that should be monitored. Changes to these settings outside normal administrative tasks can indicate illegitimate activity.

Table 2-55 Description of the **Schema Master Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory FSMO Changes
Option	Schema Master Changed
Rule Name	Schema_Master_Changed
Severity	Warning
Event IDs	565, 566, 4661, 4662
Description	Detects a change to the Active Directory FSMO schema master role.

Table 2-56 Description of the **Domain Master Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory FSMO Changes

Table 2-56 Description of the **Domain Master Changed** parameters used *(continued)*

Parameter	Description
Option	Domain Master Changed
Rule Name	Schema_Master_Changed
Severity	Warning
Event IDs	565, 566, 4661, 4662
Description	Detects a change to the Active Directory FSMO schema master role.

Table 2-57 Description of the **RID Master Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory FSMO Changes
Option	RID Master Changed
Rule Name	RID_Master_Changed
Severity	Warning
Event IDs	565, 566, 4661, 4662
Description	Detects a change to the Active Directory FSMO RID master role.

Table 2-58 Description of the **PDCEmulator Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory FSMO Changes
Option	PDCEmulator Changed
Rule Name	PDCEmulator_Changed
Severity	Warning
Event IDs	565, 566, 4661, 4662
Description	Detects a change to the Active Directory FSMO PDCEmulator.

Table 2-59 Description of the **Infrastructure Master Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Active Directory FSMO Changes
Option	Infrastructure Master Changed
Rule Name	Infrastructure_Changed
Severity	Warning
Event IDs	565, 566, 4661, 4662
Description	Detects a change to the Active Directory FSMO Infrastructure Master.

Authentication and Encryption Configuration

This option group sub-section detects normal Active Directory authentication activity as well as changes to Windows Active Directory authentication and encryption settings. Changes to these settings are normally necessary to allow non-Windows clients to access the domain. Windows writes the events to event logs, and Symantec Critical System Protection monitors the registry keys or Event IDs.

Table 2-60 Description of the **Authentication Packages Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Authentication Packages Changed
Rule Name	Authentication_Packages_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\Authentication Packages
Description	Detects the changes to the Windows authentication packages, according to the registry settings monitored.

Table 2-61 Description of the **Auth Ticket Request Failure** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Auth Ticket Request Failure
Rule Name	Auth_Ticket_Request_Failure
Severity	Notice
Event IDs	676, 672, 4772, 4768
Description	Detects the failure of Windows to receive an authentication ticket on request by Active Directory.

Table 2-62 Description of the **EnableSecuritySignature Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	EnableSecuritySignature Changed
Rule Name	EnableSecuritySignature_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanMan*\Parameters\EnableSecuritySignature
Description	Detects the changes to the Windows Security Signature state.

Table 2-63 Description of the **Kerberos Ticket Request Failed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Kerberos Ticket Request Failed
Rule Name	Kerberos_Service_Ticket_Request_Failed
Severity	Notice
Event IDs	677, 673, 4773, 4769

Table 2-63 Description of the **Kerberos Ticket Request Failed** parameters used *(continued)*

Parameter	Description
Description	Detects the failure of Windows to be granted with a Kerberos service ticket on request by an Active Directory server. This failure may happen while satisfactory security credentials are negotiated between the clients and the Active Directory server. This failure can also indicate that an untrusted client has attempted to access the resources in this Active Directory domain.

Table 2-64 Description of the **LMCompatibilityLevel Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	LMCompatibilityLevel Changed
Rule Name	LMCompatibilityLevel_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\lmcompatibilitylevel
Description	Detects the failure of Windows to be granted with a Kerberos service ticket on request by an Active Directory server. This failure may happen while satisfactory security credentials are negotiated between the clients and the Active Directory server. This failure can also indicate that an untrusted client has attempted to access the resources in this Active Directory domain.

Table 2-65 Description of the **NotificationPackages Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	NotificationPackages Changed
Rule Name	NotificationPackages_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\Notification Packages

Table 2-65 Description of the **NotificationPackages Changed** parameters used *(continued)*

Parameter	Description
Description	Detects the changes in the state of the Windows Local Security Authority Notification Packages.

Table 2-66 Description of the **Pre Authentication Failure** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Pre Authentication Failure
Rule Name	Pre_Authentication_Failure
Severity	Warning
Event IDs	675, 4771
Description	Detects the failure of Windows to pre-authenticate with Active Directory. This event happens while satisfactory security credentials are negotiated between the clients and Active Directory server. This detection can also indicate that an untrusted client has attempted to access the resources in this Active Directory domain.

Table 2-67 Description of the **RequireSecureSign Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	RequireSecureSign Changed
Rule Name	RequireSecureSign_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanMan*\Parameters\RequireSecuritySignature
Description	Detects the changes in the Windows Lan Manager Security Signature requirement.

Table 2-68 Description of the **RestrictNullSessAccess Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	RestrictNullSessAccess Changed
Rule Name	RestrictNullSessAccess_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\RestrictNullSessAccess
Description	Detects the changes in the Windows Null Session Access restrictions.

Table 2-69 Description of the **Authentication Ticket Granted** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Authentication Ticket Granted
Rule Name	Authentication_Ticket_Granted
Severity	Notice
Event IDs	672, 4768
Description	Detects when an Active Directory server grants an authentication ticket to a computer that runs Windows. This behavior is normal and often indicates that a domain user has logged on to a Windows client.

Table 2-70 Description of the **Kerberos Policy Changed** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Kerberos Policy Changed
Rule Name	Kerberos_Policy_Changed
Severity	Notice

Table 2-70 Description of the **Kerberos Policy Changed** parameters used *(continued)*

Parameter	Description
Event IDs	617, 4713
Description	Detects the updates to the Kerberos authentication policy. This normal activity occurs at 5-minute intervals when the domain group policy object is updated every 16 hours, regardless of the following items: ■ Policy object status ■ When the group policies are manually propagated

Table 2-71 Description of the **Kerberos Service Ticket Granted** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Kerberos Service Ticket Granted
Rule Name	Kerberos_Service_Ticket_Granted
Severity	Notice
Event IDs	673, 4769
Description	Detects the grant of a Kerberos service ticket to Windows by Active Directory. This event indicates that a client has been granted permission to interact in this Active Directory domain.

Table 2-72 Description of the T**rusted Logon Process Register** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Trusted Logon Process Register
Rule Name	Trusted_Logon_Process_Register
Severity	Notice
Event IDs	515, 4611

Table 2-72 Description of the T**rusted Logon Process Register** parameters used *(continued)*

Parameter	Description
Description	Detects the Windows registration of a trusted logon process to the Local Security Authority.

Table 2-73 Description of the **Encrypted Data Policy Change** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Encrypted Data Policy Change
Rule Name	Encrypted_Data_Policy_Change
Severity	Notice
Event IDs	618, 4614
Description	Detects the changes to the encrypted data recovery policy.

Table 2-74 Description of the **Quality Service Policy Changes** parameters used

Parameter	Description
Option Path	System Active Directory Change Monitor > Authentication and Encryption Configuration
Option	Quality Service Policy Changes
Rule Name	Quality_Service_Policy_Changed
Severity	Notice
Event IDs	619, 4615
Description	Detects the changes to the quality of service policy.

System Login Activity and Access Monitor

This option group section of the policy monitors the system access activity that may indicate illegitimate activity. Portions of this section also monitor the successful logon attempts of individuals through various means. These monitoring areas can be used for the following tasks:

- To acquire a timeline of when an individual logon to a specific system has occurred.
- To detect other suspicious system access activity.
- To alert on brute force password attempts.

System Login Success Monitor

This option group subsection monitors for successful logons by using various means of remote desktop, FTP, and logon attempts based on user-defined non-working hours. You can match these rules with System Logoff Monitoring to formulate a time line of individual logon activity.

Table 2-75 Description of the **Account Used for Logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	Account Used for Logon
Rule Name	Account_Used_for_Logon
Severity	Notice
Event IDs	680, 4776
Description	Detects the account that was used for the logon. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that an account has been used to log on, it reports this event.

Table 2-76 Description of the **By Admin to Desktop** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	By Admin to Desktop
Rule Name	Successful_Login_Admin_to_Desktop
Severity	Notice
Event IDs	528, 4624

Table 2-76 Description of the **By Admin to Desktop** parameters used *(continued)*

Parameter	Description
Description	Detects a successful administrator logon to a system's desktop, including local and terminal service logons. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the Windows Security Policy auditing system determines that an administrator successfully logged on, it reports this event.

Table 2-77 Description of the **by Admin via Remote Connection** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	by Admin via Remote Connection
Rule Name	Successful_Login_Admin_via_Remote_Connection
Severity	Notice
Event IDs	528, 540, 4624
Description	Detects a successful administrator logon from a shared network resource, for example, IIS, FTP, or Telnet. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that an administrator successfully logged on from a remote connection, it reports this event.

Table 2-78 Description of the **by Anonymous to IIS or FTP** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	by Anonymous to IIS or FTP
Rule Name	Successful_Login_Anon_to_IIS_or_FTP
Severity	Notice
Event IDs	528, 540, 4624, 4636

Table 2-78 Description of the **by Anonymous to IIS or FTP** parameters used *(continued)*

Parameter	Description
Description	Detects a successful anonymous access by IIS or FTP. This rule triggers only during the initial access to the Web site by any browser. If Web traffic is sporadic, the inactive connection time expires the logon.

Table 2-79 Description of the **by Guest to Desktop** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	by Guest to Desktop
Rule Name	Successful_Login_Guest_to_Desktop
Severity	Notice
Event IDs	528, 4624
Description	Detects a successful guest logon to a system's desktop. This detection includes local logons and terminal service logons. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that a guest successfully logged on, it reports this event.

Table 2-80 Description of the **by Guest via Remote Connection** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	by Guest via Remote Connection
Rule Name	Successful_Login_Guest_via_Remote_Connection
Severity	Notice
Event IDs	528, 540, 4624, 4636

Table 2-80 Description of the **by Guest via Remote Connection** parameters used *(continued)*

Parameter	Description
Description	Detects a successful guest logon by a shared network resource, for example, IIS, FTP, or Telnet. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When it determines that a guest successfully logged on by a remote connection, it reports this event

Table 2-81 Description of the **by User to Desktop** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	by User to Desktop
Rule Name	Successful_Login_User_to_Desktop
Severity	Notice
Event IDs	528, 4624
Description	Detects a successful user logon to a system's Desktop, including local logons and terminal service logons. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the Windows Security Policy auditing system determines that a user successfully logged on, it reports this event.

Table 2-82 Description of the **by User via Remote Connection** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	by User via Remote Connection
Rule Name	Successful_Login_User_via_Remote_Connection
Severity	Notice
Event IDs	528, 540, 4624, 4636

Table 2-82 Description of the **by User via Remote Connection** parameters used *(continued)*

Parameter	Description
Description	Detects a successful user logon by a shared network resource, for example, IIS, FTP, or Telnet. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When it determines that a user has logged on by a remote connection, it reports this event.

Table 2-83 Description of the Non Working Hours Rules Login Success parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	Non Working Hours Rules Login Success
Rule Name	System_Unlocked_After_Hours
Severity	Warning
Event IDs	528, 4624
Description	Detects when a system desktop is unlocked after normal business hours. By default, after business hours is defined as Monday through Friday from 7:00 P.M. to 6:00 A.M. You can configure the Windows Security Policy auditing system to monitor the status of unlocking events. When the Windows Security Policy auditing system determines that a user successfully unlocked the workstation outside of normal working hours, it reports this event.

Table 2-84 Description of the **System Unlocked During Weekends** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor
Option	System Unlocked During Weekends
Rule Name	System_Unlocked_During_Weekends
Severity	Warning
Event IDs	528, 4624

Table 2-84 Description of the **System Unlocked During Weekends** parameters used *(continued)*

Parameter	Description
Description	Detects when a system desktop is unlocked during weekends. By default, weekend is defined as Friday 7:00 P.M. to Monday 6:00 A.M. You can configure the Windows Security Policy auditing system to monitor the status of unlocking events. When the Windows Security Policy auditing system determines that a user successfully unlocked the workstation outside of normal working hours, it reports this event.

System Logoff Monitor

This portion of the policy detects all successful Windows logoff events. You can acquire individual user logon times from the events that this portion of the policy generates. Acquire these times by comparing the logoff events with successful logon events.

Table 2-85 Description of the **by Admin** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Logoff Monitor
Option	by Admin
Rule Name	Logoff_by_Admin
Severity	Warning
Event IDs	538, 4634, 4647
Description	Detects that an administrator has successfully logged off a system from a remote location. You can configure the Windows Security Policy auditing system to monitor the status of the logoff attempts. When the auditing system determines that an administrator successfully logged off the workstation from a local location or a remote location, it reports this event.

Table 2-86 Description of the **by Guest** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Logoff Monitor
Option	by Guest

Table 2-86 Description of the **by Guest** parameters used *(continued)*

Parameter	Description
Rule Name	Logoff_by_Guest
Severity	Notice
Event IDs	538, 4634, 4647
Description	Detects that a guest has successfully logged off a system. You can configure the Windows Security Policy auditing system to monitor the status of logoff attempts. When the auditing system determines that a guest has successfully logged off the workstation from a local location or a remote location, it reports this event.

Table 2-87 Description of the **by User** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Logoff Monitor
Option	by User
Rule Name	Logoff_by_User
Severity	Notice
Event IDs	538, 4634, 4647
Description	Detects that a user has successfully logged off a system. You can configure the Windows Security Policy auditing system to monitor the status of logoff attempts. When the auditing system determines that a user successfully logged off the workstation from a local location or a remote location, it reports this event.

Table 2-88 Description of the **by Specific User** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Logoff Monitor
Option	by Specific User
Rule Name	Logoff_by_User
Severity	Notice
Event IDs	538, 4634, 4647

Table 2-88 Description of the **by Specific User** parameters used *(continued)*

Parameter	Description
Description	Detects that a specific user-defined user or users have successfully logged off a system. You can configure the Windows Security Policy auditing system to monitor the status of logoff attempts. When the auditing system determines that a user successfully logged off the workstation from a local location or a remote location, it reports this event.

System Failed Login Monitor

This option group subsection detects when a user has failed to authenticate. That is, has failed to log on to a Windows system either as a local user or as a member of a domain. This activity most often indicates normal behavior, ranging from expired passwords to a user who forgets a current password. However, it may also indicate attempts by an unauthorized user to gain illegitimate access to the system or the domain.

Note: The first option under **System Failed Login Monitor**, **N Tries**, allows the administrator to set thresholds based alerting on all failed logon events. For example, an **N Tries** setting of 3 and an Interval of 1 minute only generates an alert if a user makes more than three failed logon attempts within the interval time of 1 minute. You can use this option to detect brute force-based credential attacks.

Table 2-89 Description of the **Account Disabled** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Account Disabled
Rule Name	Account_Disabled
Severity	Warning
Event IDs	531, 4625

Table 2-89 Description of the **Account Disabled** parameters used *(continued)*

Parameter	Description
Description	Detects when a user has failed to access the client, due to a disabled account. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon failed because the account was disabled, it reports this event.

Table 2-90 Description of the **Account Expired** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Account Expired
Rule Name	Account_Expired
Severity	Notice
Event IDs	532, 4625
Description	Detects when a user has failed to access the client, due to an expired account. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon has failed because the account has expired, it reports this event.

Table 2-91 Description of the **Account Locked Out** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Account Locked Out
Rule Name	Account_Locked_Out
Severity	Warning
Event IDs	539, 4740

Table 2-91 Description of the **Account Locked Out** parameters used *(continued)*

Parameter	Description
Description	Detects when a user has failed to access the client, due to a lock on the account. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon has failed because the account was locked out, it reports this event.

Table 2-92 Description of the **By Admin to Desktop** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	By Admin to Desktop
Rule Name	Login_Failed_Admin_to_Desktop
Severity	Warning
Event IDs	529, 4625
Description	Detects when an administrator has failed to log on to a system's desktop, either locally or by Terminal Services. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that an administrator has failed to log on to the local desktop or through the Terminal Services, it reports this event.

Table 2-93 Description of the **By Admin via Remote Connection** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	By Admin via Remote Connection
Rule Name	Login_Failed_Admin_via_Remote_Connection
Severity	Warning
Event IDs	529, 4625

Table 2-93 Description of the **By Admin via Remote Connection** parameters used *(continued)*

Parameter	Description
Description	Detects when an administrator has failed to log on to a system or to a domain on the network. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that an administrator has failed to log on through a remote connection, it reports this event.

Table 2-94 Description of the **By Guest to Desktop** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	By Guest to Desktop
Rule Name	Login_Failed_Guest_to_Desktop
Severity	Warning
Event IDs	529, 4625
Description	Detects when a guest has failed to log on to a system's desktop, either locally or by Terminal Services. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a guest has failed to log on, it reports this event.

Table 2-95 Description of the **By Guest via Remote Connection** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	By Guest via Remote Connection
Rule Name	Login_Failed_Guest_via_Remote_Connection
Severity	Warning
Event IDs	529, 4625

Table 2-95 Description of the **By Guest via Remote Connection** parameters used *(continued)*

Parameter	Description
Description	Detects when a guest has failed to log on to a system or domain on the network. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a guest has failed to log on by a remote connection, it reports this event.

Table 2-96 Description of the **By User to Desktop** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	By User to Desktop
Rule Name	Login_Failed_User_to_Desktop
Severity	Warning
Event IDs	529, 4625
Description	Detects when a user has failed to log on to a system's desktop, either locally or by Terminal Services. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a user has failed to log on to the local desktop, it reports this event.

Table 2-97 Description of the **By User via Remote Connection** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	By User via Remote Connection
Rule Name	Login_Failed_User_via_Remote_Connection
Severity	Warning
Event IDs	529, 4625

Table 2-97 Description of the **By User via Remote Connection** parameters used *(continued)*

Parameter	Description
Description	Detects when a user has failed to log on to a system or domain on the network. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a user has failed to log on by a remote connection, it reports this event.

Table 2-98 Description of the **Logon Failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Logon Failure
Rule Name	Login_Failed_Generic
Severity	Notice
Event IDs	537
Description	Detects when an unexpected error has occurred during logon. A failed authentication by a cleartext password, Windows NT Lan Manager, or Windows Kerberos security authentication system can cause this error. This detection may also indicate a failure to access the File Transfer Protocol (FTP) services that are related to the Microsoft Internet Information Server (IIS).

Table 2-99 Description of the **Logon to Account Failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Logon to Account Failure
Rule Name	Login_Failed_Generic_to_Account
Severity	Notice
Event IDs	681

Table 2-99 Description of the **Logon to Account Failure** parameters used *(continued)*

Parameter	Description
Description	Detects when a down-level client fails a logon attempt. Windows generates an error message on the Windows domain controller. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a domain logon failed, it reports this event.

Table 2-100 Description of the **Password Expired** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Password Expired
Rule Name	Password_Expired
Severity	Notice
Event IDs	535, 4625
Description	Detects when a user has failed to access a client, due to an expired account password. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that a logon failed, due to an expired account, it reports this event.

Table 2-101 Description of the **Unauthorized Access** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Unauthorized Access
Rule Name	Unauthorized_Access
Severity	Warning
Event IDs	534, 4625

Table 2-101 Description of the **Unauthorized Access** parameters used *(continued)*

Parameter	Description
Description	Detects when a user has failed to access a client because the local access rights or the remote access rights have not been granted to the user. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the auditing system determines that a logon failed due to a disabled account, it reports this event.

Table 2-102 Description of the **Unauthorized Location** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Unauthorized Location
Rule Name	Unauthorized_Location
Severity	Warning
Event IDs	533, 4625
Description	Detects when a user has failed to access to the domain because the client is not authorized to participate in the domain. You can configure the Windows Security Policy auditing system to monitor the status of the logon attempts. When the auditing system determines that a logon has failed because the logon was attempted from an unauthorized client, it reports this event.

Table 2-103 Description of the **Unauthorized Time** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor
Option	Unauthorized Time
Rule Name	Unauthorized_Time
Severity	Warning
Event IDs	530, 4625

Table 2-103 Description of the **Unauthorized Time** parameters used *(continued)*

Parameter	Description
Description	Detects when a domain user has failed to access a client, because the account is not authorized to access the domain during this time period. You can configure the Windows Security Policy auditing system to monitor the status of logon attempts. When the auditing system determines that the failure has occurred because the account was not allowed to log on during this time period, it reports this event.

System Hardening Monitor

This option group section detects changes to the user-configurable registry keys that are considered sensitive in maintaining the security posture of the operating system. Various areas are monitored to generate events for the administrator if either of the following entities changed any of the selected values:

- Malware
- A malicious individual attempting to lower the security posture of the host system

System Autorun Configuration

This option group subsection detects modifications of the system configuration that change whether it automatically runs code during system startup or from newly inserted CD-ROMs. This behavior is normal if an administrator needs to change autorun behavior. If unexpected, it can indicate that the system is being prepared to operate outside established security policy, or that it is about to be compromised.

Note: The final option set, **User Desktop Logon Check**, enables a function of these rules to only monitor and generate an event if a user is logged on.

Table 2-104 Description of the **CDROM Value Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System AutoRun Configuration
Option	CDROM Value Changed
Rule Name	CDROM_Value_Changed

Table 2-104 Description of the **CDROM Value Changed** parameters used *(continued)*

Parameter	Description
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Cdrom\Autorun
Description	Detects the changes to the CD-ROM AutoRun behavior, according to the registry setting: HKLM\System\CurrentControlSet\Services\CD-ROM key Autorun value. This value determines whether the system automatically runs code from the newly inserted CD-ROMs.

Table 2-105 Description of the **Run Key Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System AutoRun Configuration
Option	Run Key Changed
Rule Name	Run_Key_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\*
Description	Detects the changes to the Run registry key, according to the registry setting: HKLM\Software\Microsoft\Windows\CurrentVersion\Run key.

Table 2-106 Description of the **RunOnceEx Key Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System AutoRun Configuration
Option	RunOnceEx Key Changed
Rule Name	RunOnceEx_Key_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\*

Table 2-106 Description of the **RunOnceEx Key Changed** parameters used *(continued)*

Parameter	Description
Description	Detects the changes to the RunOnceEx registry key, according to the registry setting: HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx key. The system configuration has been modified to change the behavior of the system the next time a user logs on. This key allows a specified routine or a list of routines to execute once. It then clears itself so that it does not run on the next logon.

Table 2-107 Description of the **Userinit Value Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System AutoRun Configuration
Option	Userinit Value Changed
Rule Name	Userinit_Value_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
Description	Detects the changing of the Userinit key, according to registry setting: HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon key Userinit value. This key specifies the program that Winlogon runs when a user logs on. This program is typically Userinit.exe. This behavior is unusual, however. It would be expected if the system was updated to run the enterprise-unique routines first, then run the Userinit.exe or Explorer.exe.

Network Comm Configuration

This option group subsection detects changes to the various registry keys that deal with network and communication settings. This policy can be applied to any Windows server. Unauthorized or unknown network changes as monitored in this portion of the policy may indicate suspicious activity.

Table 2-108 Description of the **Autodisconnect Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > Network Comm Configuration

Table 2-108 Description of the **Autodisconnect Changed** parameters used *(continued)*

Parameter	Description
Option	Autodisconnect Changed
Rule Name	Autodisconnect_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\ Parameters\autodisconnect
Description	Detects the changes to the HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Services\LanmanServer\Parameters\autodisconnect registry key. This registry key determines the time that is allowed for an inactive connection before it is automatically disconnected.

Table 2-109 Description of the **TcpMaxDupAcks Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > Network Comm Configuration
Option	TcpMaxDupAcks Changed
Rule Name	TcpMaxDupAcks_Changed
Severity	Warning
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip\ Parameters\TcpMaxDupAcks
Description	Detects the changes to the HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDupAcks registry key. This registry key determines the number of duplicate ACKs, which must be received for the same sequence number of sent data, before a fast retransmit is triggered to resend the segment that was dropped in transit.

System File Protection Status

This option group subsection detects the events that the Windows File Protection (WFP) System reports. The WFP monitors the critical operating system files that should remain available, but should not change during the course of operation. If a monitored file is deleted or modified, or its attributes are changed, the WFP immediately restores the file to its original configuration. These events can occur for a number of reasons. The reasons include third-party software installation, system misconfiguration, or illegitimate manipulation. Activation of WFP file restoration procedures may be a response to illegitimate activity.

Table 2-110 Description of the **File Restoration Failed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Protection Status
Option	File Restoration Failed
Rule Name	File_Restoration_Failed
Severity	Critical
Event IDs	64004, 64007, 64006, 64021, 64005, 64008
Description	Detects when a file that the Windows File Protection System protects cannot be restored. The Windows File Protection System monitors the status of protected files and attempts to restore them to their original condition when it detects any changes. If the Windows File Protection System determines that it cannot successfully restore the file, it reports this error.

Table 2-111 Description of the **File Restoration Success** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Protection Status
Option	File Restoration Success
Rule Name	File_Restoration_Success
Severity	Warning
Event IDs	64000, 64003, 64019, 64020, 64001, 64002
Description	Detects when a file that the Windows File Protection System protects has been restored. The Windows File Protection System monitors the status of protected files and restores them to their original condition when it detects any changes. If the Windows File Protection System determines that it successfully restored a file, it reports this status.

Table 2-112 Description of the **WFP Errors** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Protection Status

Table 2-112 Description of the **WFP Errors** parameters used *(continued)*

Parameter	Description
Option	WFP Errors
Rule Name	WFP_Errors
Severity	Critical
Event IDs	64034, 64033, 64032
Description	Detects when the Windows File Protection System has detected a configuration error. The Windows File Protection System monitors its ability to access a protected file cache. It also monitors the active state or initialized state of the File Protection System. If the Windows File Protection System determines that it cannot access the cache, or that its state is inactive or not initialized, it reports these errors.

Table 2-113 Description of the **Scanning Started** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Protection Status
Option	Scanning Started
Rule Name	Scanning_Started
Severity	Notice
Event IDs	64016
Description	Detects when the Windows File Protection System has started a scan of critical system files. The Windows File Protection System scans the protected files to determine their condition. When the Windows File Protection System determines that it successfully started a scan, it reports this status.

Table 2-114 Description of the **Scanning Completed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Protection Status
Option	Scanning Completed
Rule Name	Scanning_Completed
Severity	Notice

Table 2-114 Description of the **Scanning Completed** parameters used *(continued)*

Parameter	Description
Event IDs	64017
Description	Detects when the Windows File Protection System has completed a scan of critical system files. The Windows File Protection System scans these protected files to determine their condition. When the Windows File Protection System determines that it successfully completed a scan, it reports this status.

Table 2-115 Description of the **Scanning Canceled** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Protection Status
Option	Scanning Canceled
Rule Name	Scanning_Canceled
Severity	Warning
Event IDs	64018
Description	Detects when a Windows File Protection System scan has been canceled. The Windows File Protection System scans these protected files to determine their condition. When the Windows File Protection System determines that a command has interrupted the scanning process, it reports this status.

System Security Configuration

This option group subsection detects changes to the various registry keys that deal with the typical security settings of a host system. These settings range from protection mode changes to how legal captions are viewed upon logon. See the individual rule description for more information.

Table 2-116 Description of the **AllocateCdroms Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	AllocateCdroms Changed
Rule Name	AllocateCdroms_Changed

Table 2-116 Description of the **AllocateCdroms Changed** parameters used *(continued)*

Parameter	Description
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon key AllocateCdroms value. This value determines whether data in the CD-ROM drive is accessible to other users.

Table 2-117 Description of the **AllocateFloppies Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	AllocateFloppies Changed
Rule Name	AllocateFloppies_Changed
Severity	Warning
Registry Keys	Warning \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key AllocateFloppies value. This value determines whether data in the floppy disk drive is accessible to other users.

Table 2-118 Description of the **AutoShareServer Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	AutoShareServer Changed
Rule Name	AutoShareServer_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\AutoShareServer

Table 2-118 Description of the **AutoShareServer Changed** parameters used *(continued)*

Parameter	Description
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters key AutoShareServer value. This value creates the administrative shares (C, D, ADMIN) for the physical drives.

Table 2-119 Description of the **AutoShareWks Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	AutoShareWks Changed
Rule Name	AutoShareWks_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\AutoShareWks
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters key AutoShareWks value. This value is responsible for enabling and disabling the automatic sharing of hidden shares.

Table 2-120 Description of the **ComSpec Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	ComSpec Changed
Rule Name	ComSpec_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session Manager\Environment\ComSpec
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment key ComSpec value. This value is responsible for defining the path to the DOS command interpreter, Command.com.

Table 2-121 Description of the **Debugger Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Debugger Changed
Rule Name	Debugger_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Debugger
Description	Detects any changes or attempted changes to the HKLM\Software\Microsoft\Windows NT\CurrentVersion\AeDebug key Debugger value. This value is responsible for determining whether to automatically spawn the Win32 debugger during an application fault.

Table 2-122 Description of the **Directory Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Directory Changed
Rule Name	Directory_Changed
Severity	Critical
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Windows\Directory
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Windows key Directory value. This value contains the information that helps to define the system directories for the Win32 subsystem.

Table 2-123 Description of the **DisableTaskMgr Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	DisableTaskMgr Changed
Rule Name	DisableTaskMgr_Changed
Severity	Warning

Table 2-123 Description of the **DisableTaskMgr Changed** parameters used *(continued)*

Parameter	Description
Registry Keys	\HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion \Policies\System\DisableTaskMgr
Description	Detects any changes or attempted changes to the HKU\Software\Microsoft\Windows\CurrentVersion\Policies\System key DisableTaskMgr value. This value controls the ability of users to start Task Manager and view processes and view running applications. It also controls the ability of users to make changes to the priority or state of the individual processes.

Table 2-124 Description of the **DontDisplayLastUserName Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	DontDisplayLastUserName Changed
Rule Name	DontDisplayLastUserName_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \policies\system\dontdisplaylastusername
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system key DontDisplayLastUserName value. If you enable this value, the user name box on the logon screen is blank . This behavior prevents the people that log on from knowing the last user to access the system.

Table 2-125 Description of the **Hidden Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Hidden Changed
Rule Name	Hidden_Changed
Severity	Warning

Table 2-125 Description of the **Hidden Changed** parameters used *(continued)*

Parameter	Description
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\hidden
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters key hidden value. This value is responsible for hiding a server from the Network Browser.

Table 2-126 Description of the **LegalNoticeText Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	LegalNoticeText Changed
Rule Name	LegalNoticeText_Changed
Severity	Info
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeText \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\LegalNoticeText
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key LegalNoticeCaption value or to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system key LegalNoticeText value. This value creates a dialog box that is presented to any users before they log onto the system.

Table 2-127 Description of the **PasswordExpiryWarning Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	PasswordExpiryWarning Changed
Rule Name	PasswordExpiryWarning_Changed
Severity	Info

Table 2-127 Description of the **PasswordExpiryWarning Changed** parameters used *(continued)*

Parameter	Description
Registry Keys	\HKEY_LOCAL_MACHINE\software\Microsoft\WindowsNT\CurrentVersion \Winlogon\PasswordExpiryWarning
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key PasswordExpiryWarning value. This value is responsible for informing users of how many days are left until their password expires.

Table 2-128 Description of the **Path Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Path Changed
Rule Name	Path_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session Manager\Environment\Path
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment key Path value. This value determines the directory search order for all open applications on your target system.

Table 2-129 Description of the **SubmitControl Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	SubmitControl Changed
Rule Name	SubmitControl_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\SubmitControl

Table 2-129 Description of the **SubmitControl Changed** parameters used *(continued)*

Parameter	Description
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Lsa key SubmitControl value. This value gives other users (e.g., Server Operators) permission to issue AT commands.

Table 2-130 Description of the **SystemDirectory Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	SystemDirectory Changed
Rule Name	SystemDirectory_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Windows\SystemDirectory
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Windows key SystemDirectory value. This value contains the entries that define the system directories for the Win32 subsystem.

Table 2-131 Description of the **Users Connect Count Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Users Connect Count Changed
Rule Name	Users_Connect_Count_Changed
Severity	Info
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\LanmanServer\Parameters\Users
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters key Users value for changes. This value is responsible for allowing more than 10 clients to connect to a computer.

Table 2-132 Description of the **VDD Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	VDD Changed
Rule Name	VDD_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\ \VirtualDeviceDrivers\VDD
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\VirtualDeviceDrivers key VDD value. This value is responsible for determining which virtual device drivers are used on program install.

Table 2-133 Description of the **AddPrintDrivers Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	AddPrintDrivers Changed
Rule Name	AddPrintDrivers_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Print\Providers\ LanMan Print Services\Servers\AddPrinterDrivers
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers key AddPrinterDrivers value. This value restricts the installation of printer drivers to only Administrators and Print Operators.

Table 2-134 Description of the **RestrictAnonymous Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	RestrictAnonymous Changed
Rule Name	RestrictAnonymnus_Changed

Table 2-134 Description of the **RestrictAnonymous Changed** parameters used *(continued)*

Parameter	Description
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\RestrictAnonymous
Description	Detects any changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous key. This value is responsible for restricting who has access to the registry.

Table 2-135 Description of the **Driver Signing Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Driver Signing Changed
Rule Name	Driver_Signing_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing\Policy
Description	Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing key Policy value. This value is responsible for determining what to do when an attempt is made to install a driver without a valid Catalog file.

Table 2-136 Description of the **Non Driver Signing Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Non Driver Signing Changed
Rule Name	Non_Driver_Signing_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-DriverSigning\Policy

Table 2-136 Description of the **Non Driver Signing Changed** parameters used *(continued)*

Parameter	Description
Description	Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing key Policy value. This value is responsible for allowing unsigned drivers to be installed.

Table 2-137 Description of the **Local Auto Logoff Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Local Auto Logoff Changed
Rule Name	Local_Auto_Logoff_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\lanmanserver\parameters\enableforcedlogoff
Description	Detects any changes or attempted changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\enableforcedlogoff key. This key is responsible for automatically logging off users when logon time expires (local).

Table 2-138 Description of the **FullPrivilegeAuditing Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	FullPrivilegeAuditing Changed
Rule Name	FullPrivilegeAuditing_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Lsa\fullprivilegeauditing
Description	Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa key fullprivilegeauditing value. This value is responsible for the Backup and Restore privileges in the user rights audit class.

Table 2-139 Description of the **SmartCard Behavior Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	SmartCard Behavior Changed
Rule Name	SmartCard_Behavior_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\scremoveoption
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key scremoveoption value. This value locks the computer when a smart card is removed.

Table 2-140 Description of the **Recovery Console Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Recovery Console Changed
Rule Name	Recovery_Console_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Setup\RecoveryConsole\*
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel and SetCommand keys. These keys determine if the Recovery Console is to be used when Windows crashes.

Table 2-141 Description of the **NTFS MediaEject Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	NTFS MediaEject Changed
Rule Name	NTFS_MediaEject_Changed
Severity	Warning

Table 2-141 Description of the **NTFS MediaEject Changed** parameters used *(continued)*

Parameter	Description
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\allocatedasd
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\allocatedasd key. This value determines whether the ability to access removable drives is available to other users.

Table 2-142 Description of the **CTRL ALT DEL for Logon Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	CTRL ALT DEL for Logon Changed
Rule Name	CTRL_ALT_DEL_for_Logon_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \policies\system\disablecad
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system key disablecad. This value controls whether users are required to press Ctrl + Alt + Delete before logging into the system.

Table 2-143 Description of the **Protection Mode Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Protection Mode Changed
Rule Name	Protection_Mode_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control \Session Manager\ProtectionMode

Table 2-143 Description of the **Protection Mode Changed** parameters used *(continued)*

Parameter	Description
Description	Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Control\Session Manager\ProtectionMode key. This key is responsible for strengthening default permissions of global system objects.

Table 2-144 Description of the **Plaintext Password Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Plaintext Password Changed
Rule Name	Plaintext_Password_Changed
Severity	Warning
Registry Keys	HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\ lanmanworkstation\parameters\enableplaintextpassword
Description	Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Services\lanmanworkstation\ parametersenableplaintextpassword key. This key enables unencrypted passwords to connect to third-party SMB servers.

Table 2-145 Description of the **CrashOnAuditFail Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	CrashOnAuditFail Changed
Rule Name	CrashOnAuditFail_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control \Lsa\crashonauditfail
Description	Detects any changes or attempted changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa key crashonauditfail value. This value determines system behavior when the Security log (Event Viewer) is full.

Table 2-146 Description of the **Sys Maintenance RegKey Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Sys Maintenance RegKey Changed
Rule Name	Sys_Maintenance_RegKey_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Netlogon \Parameters\DisablePasswordChange
Description	Detects any changes to the HKEY_LOCAL_MACHINE SYSTEM\CurrentControlSet\Services\Netlogon\ ParametersDisablePasswordChange key. This key enables system maintenance of account passwords.

Table 2-147 Description of the **Secure Channel Sign RegKey Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Secure Channel Sign RegKey Changed
Rule Name	Secure_Ch_Sign_Regkey_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Netlogon \Parameters\signsecurechannel
Description	Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon \Parameters\signsecurechannel key. This key determines whether or not you require Secure Channel to digitally sign secure channel data, when possible.

Table 2-148 Description of the **Secure Channel Always RegKey Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration

Table 2-148 Description of the **Secure Channel Always RegKey Changed** parameters used *(continued)*

Parameter	Description
Option	Secure Channel Always RegKey Changed
Rule Name	Secure_Ch_Always_Regkey_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Netlogon \Parameters\requiresecurechannel
Description	Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\ Parameters\requiresignorseal key. This key determines whether or not you always require Secure Channel to digitally encrypt or sign secure channel data.

Table 2-149 Description of the **Secure Channel Strong RegKey Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	Secure Channel Strong RegKey Changed
Rule Name	Secure_Ch_Strong_Regkey_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Netlogon \Parameters\requirestrongkey
Description	Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon \Parameters\requirestrongkey key. This key determines whether or not you require Secure Channel to require strong session key.

Table 2-150 Description of the parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Security Configuration
Option	SecureChannel Encrypt Required RegKey Changed
Rule Name	SecureCh_Encrypt_RegKey_Changed

Table 2-150 Description of the parameters used *(continued)*

Parameter	Description
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Netlogon \Parameters\sealsecurechannel
Description	Detects any changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon \Parameters\sealsecurechannel key. This key determines whether or not you require Secure Channel to digitally encrypt secure channel data, when possible.

System StartStop Options

This option group subsection detects changes to the various registry keys that deal with typical startup and shutdown settings. See the rule descriptions for further information on rule function.

Table 2-151 Description of the **BootExecute Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	BootExecute Changed
Rule Name	BootExecute_Changed
Severity	Critical
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session Manager\BootExecute
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager key BootExecute value. This value contains the names and arguments of programs that the Session Manager executes.

Table 2-152 Description of the **CacheLogonsCount Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	CacheLogonsCount Changed

Table 2-152 Description of the **CacheLogonsCount Changed** parameters used *(continued)*

Parameter	Description
Rule Name	CacheLogonsCount_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscount
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon key CachedLogonsCount value. This value controls the number of allowable cached logon attempts when the domain controller is unavailable.

Table 2-153 Description of the **ClearPageFileAtShutdown Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	ClearPageFileAtShutdown Changed
Rule Name	ClearPageFileAtShutdown_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session Manager\Memory Management\ClearPageFileAtShutdown
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management key ClearPageFileAtShutdown value. This value determines whether Windows should clear the page file when the system is shut down.

Table 2-154 Description of the **PendingFileRenames Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	PendingFileRenames Changed
Rule Name	PendingFileRenames_Changed

Table 2-154 Description of the **PendingFileRenames Changed** parameters used *(continued)*

Parameter	Description
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session Manager\FileRenameOperations\PendingFileRenameOperations
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager \FileRenameOperations key and the PendingFileRenameOperations value. This value determines which operations are run at system shutdown.

Table 2-155 Description of the **ReportBootOK Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	ReportBootOK_Changed
Rule Name	ReportBootOK Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ReportBootOk
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key ReportBootOK value. This value helps to determine the meaning of the ControlSet.

Table 2-156 Description of the **ShutdownWithoutLogon Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	ShutdownWithoutLogon Changed
Rule Name	ShutdownWithoutLogon_Changed
Severity	Warning

Table 2-156 Description of the **ShutdownWithoutLogon Changed** parameters used *(continued)*

Parameter	Description
Registry Keys	\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon
Description	Detects any changes or attempted changes to the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key ShutdownWithoutLogon value. This value determines whether you can shut down a system without logging on.

Table 2-157 Description of the **SystemStartOptions Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System StartStop Options
Option	SystemStartOptions Changed
Rule Name	SystemStartOptions_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control \SystemStartOptions
Description	Detects any changes or attempted changes to the HKLM\SYSTEM\CurrentControlSet\Control key SystemStartOptions value. This value contains the text of system arguments that are passed to the system by the firmware. These values can be used to determine whether the debugger is enabled, the options that are set for ports and speed, and other configuration parameters.

System Audit Tampering

This option group subsection detects system auditing changes and the clearing of audit logs, which may be indicative of malicious activity or internal policy violation. The clearing of audit logs without legitimate intent is usually a sign of a malicious user or program attempting to hide its behavior.

Note: The first option, **Enable Date Restriction in Rule(s)**, provides the ability to only generate events in this section of the policy during a specific time window. This option provides tuning capabilities to monitor at specific times of the day that would make an administrator more suspicious of audit log mismanagement. For example, you would be more suspicious of such activity during non-business hours.

Table 2-158 Description of the **Audit Policy Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Audit Policy Changed
Rule Name	Audit_Policy_Changed
Severity	Warning
Description	Detects the changes to the system audit policy. See User Manager > Policies > Audit. The Windows operating system determines when the status of the auditing system has changed. When Windows determines the Audit Policy has changed, it reports the event.

Table 2-159 Description of the **Auditing Turned Off** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Auditing Turned Off
Rule Name	Auditing_Turned_Off
Severity	Critical
Description	Detects Windows auditing being turned off. The Windows operating system determines when the status of the auditing system has changed. When Windows determines the auditing system has been turned off, it reports this event.

Table 2-160 Description of the **Auditing Turned On** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Auditing Turned On

Table 2-160 Description of the **Auditing Turned On** parameters used *(continued)*

Parameter	Description
Rule Name	Auditing_Turned_On
Severity	Warning
Description	Detects Windows when the auditing system has been turned on. The Windows operating system determines when the status of the auditing system has changed. When Windows determines that the auditing system has been turned on, it reports this event.

Table 2-161 Description of the **Data Retention Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Data Retention Changed
Rule Name	Data_Retention_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services \EventLog*\Retention
Description	Detects the changes or attempted changes to the Retention value of the HKLM\System\CurrentControlSet\Services\EventLog\Application or System or Security" key. This value determines the number of days for which audit logs are retained.

Table 2-162 Description of the **Security Log Events Deleted** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Security Log Events Deleted
Rule Name	Security_Log_Events_Deleted
Severity	Critical
Event IDs	517, 1102

Table 2-162 Description of the **Security Log Events Deleted** parameters used *(continued)*

Parameter	Description
Description	Detects the clearing of security events from the Windows Event Viewer. The Windows operating system determines when the status of the auditing system has changed. When Windows determines that the security events log has been cleared, it reports this event.

Table 2-163 Description of the **Log File Size Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Log File Size Changed
Rule Name	Log_File_Size_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\EventLog\*\MaxSize
Description	Detects the changes or attempted changes to the MaxSize value of the HKLM\System\CurrentControlSet\Services\EventLog\Application or System or Security key. This value determines the maximum size of the audit log.

Table 2-164 Description of the **Log File Location Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Log File Location Changed
Rule Name	Log_File_Location_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\EventLog\*\File
Description	Detects the changes or attempted changes to the File value of the HKLM\System\CurrentControlSet\Services\EventLog\Application or System or Security key. This value determines to which file the event log is written.

Table 2-165 Description of the **Audit Changed thru HiddenKey** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Audit Tampering
Option	Audit Changed thru HiddenKey
Rule Name	Audit_Changed_thru_HiddenKey
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\Security\Policy\PolAdtEv\*
Description	Detects the changes or attempted changes to HKLM\Security\Policy\PolAdtEv key. This value controls the auditing policy of the OS when it is read on an interval timeline.

System Hardening Network Configuration

This option group subsection detects changes to the user-configured registry keys that affect the way the operating system handles various forms of network traffic. Changes to these areas may lower the security posture of the host system.

Table 2-166 Description of the **EnableICMPRedirect Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Hardening Network Configuration
Option	EnableICMPRedirect Changed
Rule Name	EnableICMPRedirect_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip \Parameters\EnableICMPRedirect \HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip \Parameters\EnableICMPRedirects
Description	Detects the changes to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip \Parameters key EnableICMPRedirect value. This value controls whether Windows alters its route table in response to ICMP redirect messages.

Table 2-167 Description of the **KeepAliveTime Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Hardening Network Configuration
Option	KeepAliveTime Changed
Rule Name	KeepAliveTime_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip \Parameters\KeepAliveTime
Description	Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \Tcpip\Parameters key KeepAliveTime value. This value specifies the idle time of the connection in milliseconds, before the TCP begins sending the keepalives, if keepalives are enabled on the connection.

Table 2-168 Description of the **PerformRouterDiscover Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Hardening Network Configuration
Option	PerformRouterDiscover Changed
Rule Name	PerformRouterDiscover_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip \Parameters\PerformRouterDiscovery
Description	Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \Tcpip\Parameters key PerformRouterDiscovery value. This value determines whether the ICMP Router Discovery Protocol is enabled, disabled, or enabled only if the DHCP sends the router discovery option.

Table 2-169 Description of the **SynAttackProtect Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Hardening Network Configuration
Option	SynAttackProtect Changed
Rule Name	SynAttackProtect_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip\Parameters\SynAttackProtect
Description	Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters key SynAttackProtect value. This value controls the protection level for your computer against any SYN attacks.

Table 2-170 Description of the **TcpMaxHalfOpen Changed** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Hardening Network Configuration
Option	TcpMaxHalfOpen Changed
Rule Name	TcpMaxHalfOpen_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip\Parameters\TcpMaxHalfOpen
Description	Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters key TcpMaxHalfOpen value. This value controls the number of connections in the SYN-RCVD state that are allowed before the SYN-ATTACK protection begins to operate.

Table 2-171 Description of the **TcpMaxHalfOpenRetried** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Hardening Network Configuration

Table 2-171 Description of the **TcpMaxHalfOpenRetried** parameters used *(continued)*

Parameter	Description
Option	TcpMaxHalfOpenRetried Changed
Rule Name	TcpMaxHalfOpenRetried_Changed
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services\Tcpip \Parameters\TcpMaxHalfOpenRetried
Description	Detects the changes to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \Tcpip\Parameters key TcpMaxHalfOpenRetried value. This value controls the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN, before the SYN-ATTACK attack protection begins to operate.

System File and Directory Monitor

This option group section of the policy monitors for file and directory changes as well as for Windows share volume creation and deletion. It also includes a completely rewritten file monitoring area that was renamed System FileWatch Monitor. This new area provides enhanced configuration options to enable more precise monitoring of file and directory additions, deletions, modifications, and access attempts.

System File Shares Configuration Monitor

This option group section of the policy monitors file share creation and deletion. Unauthorized file share creation and deletion can indicate malicious activity or possible malware activity. In addition, the creation of unauthorized or unknown file shares on host systems may lower their security posture.

Table 2-172 Description of the **System Share Creation** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Shares Configuration Monitor
Option	System Share Creation
Rule Name	Share_Creation

Table 2-172 Description of the **System Share Creation** parameters used *(continued)*

Parameter	Description
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services \LanmanServer\Shares\*
Description	Detects the creation of values under the HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares key. This value determines whether a shared drive or folder is created on the system.

Table 2-173 Description of the **System Share Deletion** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System File Shares Configuration Monitor
Option	System Share Deletion
Rule Name	Share_deletion
Severity	Warning
Registry Keys	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Services \LanmanServer\Shares\*
Description	Detects the deletion of values under the HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares key. This value determines whether a shared drive or folder is deleted on the system.

System FileWatch Monitor

This option group section of the policy monitors additions, deletions, modifications, and access attempts to the system critical files that are listed as monitored files. If you use a default security posture, then Symantec Critical System Protection automatically sets up the filewatch monitor for you. If you use your own security posture, you must select the files that you want to monitor so that the filewatch monitor functions correctly.

A wide range of options that enable very specific tuning of how the file or directory is monitored are available for each rule. A global settings area sets the following parameters for all rules in the filewatch monitor area:

- Polling Interval: The interval in which the file watch engine polls or checks the files that are configured for change monitoring. This option is available to enable tuning of how frequently files are polled for changes. You may want to adjust the default polling rate if your environment has a large number of files to be monitored. This adjustment helps to ensure that resources are not overly used for the filewatch engine. A drop-down selection criteria area is provided to easily switch polling interval frequency.
- Search Depth: The search depth is a configurable parameter. It specifies the recursion level, or number of directories and subdirectories that are monitored when you apply a wildcard path. For more information on recursion level and search depth, see the path to the existing definition.

A **Monitor File Checksums** option is available under the **Monitor File Modification** option for each type of file watched. This option enables the monitoring of a file's checksum during a file modification event. It reports the real-time SHA-256 hash comparison to the Symantec Critical System Protection console under the **Event details**. This option also enables the monitoring of file checksums as calculated at agent startup. It determines whether the file was modified since Symantec Critical System Protection was last shut down. This option provides detection ability even if the Symantec Critical System Protection service or daemon is shut down. If a monitored file is changed, once the Symantec Critical System Protection service or daemon is started, it compares the files in its monitored list to when it was shut down. Any differences are reported to the console.

For more information, see the file monitoring enhancements section of the Release Notes for Symantec Critical System Protection Version 5.2.6.

Table 2-174 Description of the **Dll Cache Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Dll Cache Files
Rule Name	Baseline_FileWatch_Sys_Dll_Cache_Files
Severity	Warning
Monitor Paths	%SystemRoot%\System32\dllcache\*.cpl %SystemRoot%\System32\dllcache\*.dll %SystemRoot%\System32\dllcache\*.exe %SystemRoot%\System32\dllcache\*.ocx %SystemRoot%\System32\dllcache\*.sys

Table 2-174 Description of the **Dll Cache Files** parameters used *(continued)*

Parameter	Description
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor the DLL cache files that the system maintains. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-175 Description of the **Driver Cache Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Driver Cache Files
Rule Name	Baseline_Filewatch_Sys_DriverCache_Files
Severity	Warning
Monitor Paths	%SystemRoot%\Driver Cache*
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor the driver cache files that the system maintains. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-176 Description of the **Security Database Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Security Database Files
Rule Name	Baseline_FileWatch_Sys_SecurityDB_Files
Severity	Warning
Monitor Paths	%SystemRoot%\security\templates\*.inf %SystemRoot%\security\database\*.sdb
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor the security database files that the system maintains. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-177 Description of the **Core System Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Core System Files
Rule Name	Baseline_FileWatch_Sys_SecurityDB_Files
Severity	Warning

Table 2-177 Description of the **Core System Files** parameters used *(continued)*

Parameter	Description
Monitor Paths	%ProgramFiles%\windows nt*.dll %ProgramFiles%\windows nt*.exe %ProgramFiles%\windows nt\accessories\*.exe %SystemRoot%*.dll %SystemRoot%*.exe %SystemRoot%\System32\*.acm %SystemRoot%\System32\*.ax %SystemRoot%\System32\*.com %SystemRoot%\System32\*.cpl %SystemRoot%\System32\*.dll %SystemRoot%\System32\*.drv %SystemRoot%\System32\*.exe %SystemRoot%\System32\*.ocx %SystemRoot%\System32\*.scr %SystemRoot%\System32\*.sys %SystemRoot%\System32\drivers\*.dll %SystemRoot%\System32\drivers\*.sys %SystemRoot%\System32\dsound.vxd %SystemRoot%\system\*.dll %SystemRoot%\system\*.drv
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-177 Description of the **Core System Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor Core System Executable Files. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-178 Description of the **Core System Configuration Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Core System Configuration Files
Rule Name	Baseline_FileWatch_Sys_Core_Configuration_Files
Severity	Warning
Monitor Paths	%SystemRoot%\System32\AUTOEXEC.NT %SystemRoot%\System32\CONFIG.NT %SystemRoot%\System32\desktop.ini %SystemRoot%\desktop.ini %SystemRoot%\system.ini %SystemRoot%\win.ini
Monitor Ops	Deleted, Created, Modified
Report File Differences	Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor Core System Configuration Files. **Note:** You enable the Report File Differences option in this portion of the filewatch rule set. This option provides a good example of specific ini files. In them, reporting differences, such as strings that are removed or added, let you determine if the event should be escalated for investigation.

Table 2-179 Description of the **Setup Dlls & Binaries** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Setup Dlls & Binaries
Rule Name	Baseline_FileWatch_Sys_Setup_Files
Severity	Warning
Monitor Paths	%SystemRoot%\System32\Setup\*.dll %SystemRoot%\System32\Setup\*.exe
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor setup DLLs & binaries. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-180 Description of the **System WBEM Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	System WBEM Files
Rule Name	Baseline_FileWatch_Sys_WBEM_Files
Severity	Warning
Monitor Paths	%SystemRoot%\System32\wbem\*.dll %SystemRoot%\System32\wbem\*.exe
Monitor Ops	Deleted, Created, Modified

Table 2-180 Description of the **System WBEM Files** parameters used *(continued)*

Parameter	Description
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor System WBEM Files. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-181 Description of the **System Export Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	System Export Files
Rule Name	Baseline_FileWatch_Sys_Export_Files
Severity	Warning
Monitor Paths	%SystemRoot%\System32\export\*.dll %SystemRoot%\System32\export\*.exe
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor System Export Files. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-182 Description of the **System OLE Support files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	System OLE Support files
Rule Name	Baseline_FileWatch_Sys_OLESupport_Files
Severity	Warning
Monitor Paths	%CommonProgramFiles%\system\ole db*.dll %CommonProgramFiles%\system\ole db*.dll %CommonProgramFiles%\system\msadc\*.dll
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor OLE Support Files. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-183 Description of the **Common Program Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Common Program Files
Rule Name	Baseline_FileWatch_Sys_Common_Program_Files
Severity	Warning
Monitor Paths	%CommonProgramFiles%\system\*.dll
Monitor Ops	Deleted, Created, Modified

Table 2-183 Description of the **Common Program Files** parameters used *(continued)*

Parameter	Description
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor Common Program Files. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-184 Description of the **Group Policy Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Group Policy Files
Rule Name	Baseline_FileWatch_Sys_Group_Policy_Files
Severity	Warning
Monitor Paths	%SystemRoot%\System32\GroupPolicy\gpt.ini %SystemRoot%\System32\GroupPolicy\Machine\Scripts\* %SystemRoot%\System32\GroupPolicy\Machine\Registry.pol %SystemRoot%\System32\GroupPolicy\User\Scripts\*
Monitor Ops	Created, Accessed, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-184 Description of the **Group Policy Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor Group Policy Files. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-185 Description of the **System IME Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	System IME Files
Rule Name	Baseline_FileWatch_Sys_IME_Files
Severity	Warning
Monitor Paths	%SystemRoot%\ime\*.dll %SystemRoot%\ime\chsime\applets\*.dll %SystemRoot%\ime\chtime\applets\*.dll %SystemRoot%\ime\shared\*.dll %SystemRoot%\ime\shared\*.dll %SystemRoot%\ime\shared\res\*.dll %SystemRoot%\ime\imjp?_1\*.dll %SystemRoot%\ime\imjp?_1\*.exe %SystemRoot%\ime\imjp?_1\applets\*.dll
Monitor Ops	Created, Delete, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-185 Description of the **System IME Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor system IME Files. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-186 Description of the **Monitor Script Files in System Folders** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Monitor Script Files in System Folders
Rule Name	Baseline_FileWatch_Sys_Script_Files
Severity	Warning
Monitor Paths	%SystemRoot%*.js %SystemRoot%*.vbs %SystemRoot%\System32\*.js %SystemRoot%\System32\*.vbs
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor Script Files, for example, JavaScript and VBScript files. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-187 Description of the **Other Files (All Windows)** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Other Files (All Windows)
Rule Name	Baseline_FileWatch_Sys_Other_Files_All_Windows
Severity	Warning
Monitor Paths	%SystemRoot%\apppatch\*.dll %SystemRoot%\System32\os2\dll\*.dll %SystemRoot%\System32\CertSrv\cafixweb.exe %SystemRoot%\System32\spool\drivers\w32x86\*
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor Other Critical System Files that are not included in any of the previous groups. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-188 Description of the **Other Files (Not in NT)** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Other Files (Not in NT)
Rule Name	Baseline_FileWatch_Sys_Other_Files_Not_NT
Severity	Warning

Table 2-188 Description of the **Other Files (Not in NT)** parameters used *(continued)*

Parameter	Description
Monitor Paths	%SystemRoot%\msagent\*.dll %SystemRoot%\msagent\*.exe %SystemRoot%\msagent\intl\*.dll %SystemRoot%\srchasst\msgr3en.dll %SystemRoot%\srchasst\srchctls.dll %SystemRoot%\pchealth\helpctr\binaries\*.dll %SystemRoot%\pchealth\helpctr\binaries\*.exe %SystemRoot%\pchealth\uploadlb\binaries\*.exe %SystemRoot%\System32\ShellExt\* %SystemRoot%\System32\Microsoft\Crypto\* %SystemRoot%\System32\Microsoft\Protect\* %SystemRoot%\System32\rpcproxy
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor Other Critical System Files that are not present in NT and that are not included in any of the previous groups. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-189 Description of the **Other Files (NT Only)** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor
Option	Other Files (NT Only)

Table 2-189 Description of the **Other Files (NT Only)** parameters used *(continued)*

Parameter	Description
Rule Name	Baseline_FileWatch_Sys_Other_Files_NT_Only
Severity	Warning
Monitor Paths	%SystemRoot%\System32\viewers\*.dll %SystemRoot%\System32\viewers\*.exe
Monitor Ops	Deleted, Created, Modified
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor Other Critical System Files that are not present in NT and that are not included in any of the previous groups. Symantec recommends that you only use the Report File Differences option on a select number of files. Enabling the reporting of file differences for a very large number of files, that is, more than 1000, may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

System Registry Monitor

This option group section monitors addition, deletion, and modification attempts to critical Windows registry locations that are listed as monitored areas within this option group. If you use a default security posture, Symantec Critical System Protection automatically sets up the registry monitor for you. If you use your own security posture, you must select the registry paths that you want to monitor so that the registry monitor functions correctly.

A wide range of options are available for each rule to enable very specific tuning of how the registry entries are monitored.

System Registry Monitor - AutoStart Keys

This subsection area of the policy monitors critical system auto start locations. Auto start registry key locations specify how specific software is started. Malware may also use this location to add malicious entries to auto start applications without an administrator’s knowledge.

Table 2-190 Description of the **AutoStart System Keys** parameters used

Parameter	Description
Option Path	System Registry Monitor > System Registry Monitor - AutoStart Keys
Option	AutoStart System Keys
Rule Name	Sys_AutoStart_Keys
Severity	Warning
Monitor Paths	\HKEY_LOCAL_MACHINE\Software\Classes\*\shell*\command \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\* \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\* \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run* \HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts \HKEY_USERS\*\Software\Classes\*\shell*\command \HKEY_USERS\*\Software\Microsoft\Windows NT\CurrentVersion\Windows\* \HKEY_USERS\*\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\* \HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Policies\System \HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Run* \HKEY_USERS\*\Software\Policies\Microsoft\Windows\System\Scripts
Monitor Ops	Created, Modified
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor default auto start registry key locations. **Note:** This option group is set up to be very similar to the functions available in the System FileWatch Monitor.

Table 2-191 Description of the **AutoStart System Keys** parameters used

Parameter	Description
Option Path	System Registry Monitor > System Registry Monitor - AutoStart Keys
Option	AutoStart System Keys
Rule Name	Sys_AutoStart_Service_Keys
Severity	Warning
Monitor Paths	\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW\* \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Monitor Ops	Created, Modified
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor service-specific auto start registry key locations. **Note:** This option group is set up to be very similar to the functions available in the System FileWatch Monitor.

Table 2-192 Description of the **AutoStart System CMD Keys** parameters used

Parameter	Description
Option Path	System Registry Monitor > System Registry Monitor - AutoStart Keys
Option	AutoStart System CMD Keys
Rule Name	Sys_AutoStart_Injection_Keys
Severity	Major
Monitor Paths	\HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor* \HKEY_USERS\*\Software\Microsoft\Command Processor
Monitor Ops	Created, Modified, Deleted
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor system command processor auto start registry key locations. **Note:** This option group is set up to be very similar to the functions available in the System FileWatch Monitor.

Table 2-193 Description of the **AutoStart Explorer Keys** parameters used

Parameter	Description
Option Path	System Registry Monitor > System Registry Monitor - AutoStart Keys
Option	AutoStart Explorer Keys
Rule Name	Sys_AutoStart_Explorer_Keys
Severity	Warning
Monitor Paths	\HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\ \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW\Control\Session Manager\Environment\ \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad \HKEY_USERS\.Default\Environment \HKEY_USERS\S-*-????\Environment \HKEY_USERS\S-*-???\Environment \HKEY_USERS\S-*-??\Environment \HKEY_USERS\S-*-?\Environment
Monitor Ops	Created, Modified
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor explorer environment-specific auto start registry key locations. **Note:** This option group is set up to be very similar to the functions available in the System FileWatch Monitor.

Table 2-194 Description of the **AutoStart System Injection Keys** parameters used

Parameter	Description
Option Path	System Registry Monitor > System Registry Monitor - AutoStart Keys
Option	AutoStart System Injection Keys

Table 2-194 Description of the **AutoStart System Injection Keys** parameters used *(continued)*

Parameter	Description
Rule Name	Sys_AutoStart_Injection_Keys
Severity	Major
Monitor Paths	\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects \HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
Monitor Ops	Created, Modified, Deleted
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor system injection auto start registry key locations. **Note:** This option group is set up to be very similar to the functions available in the System FileWatch Monitor.

System Symantec Software Monitor

This option group area of the policy contains monitoring functions for Symantec software. Currently the monitored ancillary applications are Symantec AntiVirus and Symantec Endpoint Security. The policy automatically detects if the host machine has Symantec AntiVirus and Symantec Endpoint Security installed. Therefore, even if both areas of monitoring are enabled, only one area detects and generates events. This behavior is to thwart double event generation, which could confuse an administrator.

Symantec AntiVirus Client Communication

This portion of the policy detects alerts from Symantec AntiVirus client installations. This policy can be applied to all Windows hosts with Symantec AntiVirus client installations.

Table 2-195 Description of the **Virus Detected** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	Virus Detected
Rule Name	Virus_Detection
Severity	Critical
Event IDs	5
Description	Detects the discovery of a virus or Trojan horse by Symantec AntiVirus. This detection indicates that malicious software has arrived at the client side by email, download, document macro, or by disk-to-disk transfer. Immediate action is usually warranted.

Table 2-196 Description of the **AntiVirus Service Stopped** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Service Stopped
Rule Name	Antivirus_Service_Stopped
Severity	Warning
Event IDs	13
Description	Detects the stopping of the Symantec AntiVirus service. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the Symantec AntiVirus service has stopped, it reports this status.

Table 2-197 Description of the **AntiVirus Service Started** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Service Started
Rule Name	Antivirus_Service_Started
Severity	Notice
Event IDs	14
Description	Detects the starting of the Symantec AntiVirus service. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the Symantec AntiVirus service has started, it reports this status.

Table 2-198 Description of the **AntiVirus Scan Started** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Scan Started
Rule Name	AntiVirus_Scan_Started
Severity	Notice
Event IDs	3
Description	Detects the starting of a manual scan of a host with Symantec Antivirus. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that it has initiated a manual scan of the host, it reports this status.

Table 2-199 Description of the **AntiVirus Scan Canceled** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Scan Canceled

Table 2-199 Description of the **AntiVirus Scan Canceled** parameters used *(continued)*

Parameter	Description
Rule Name	AntiVirus_Scan_Canceled
Severity	Warning
Event IDs	21
Description	Detects the canceling of a manual scan of a host with Symantec Antivirus. Symantec AntiVirus issues the status messages for various application conditions. When Symantec AntiVirus determines that it has been commanded to cancel a manual scan, it reports this status.

Table 2-200 Description of the **AntiVirus Scan Completed** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Scan Completed
Rule Name	AntiVirus_Scan_Completed
Severity	Warning
Event IDs	2
Description	Detects the completion of a manual scan of a host with Symantec Antivirus. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that it has successfully completed a manual scan, it reports this status.

Table 2-201 Description of the **New Virus Definition Loaded** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	New Virus Definition Loaded
Rule Name	New_Virus_Defintion_Loaded
Severity	Notice

Table 2-201 Description of the **New Virus Definition Loaded** parameters used *(continued)*

Parameter	Description
Event IDs	7
Description	Detects the updating of Symantec Antivirus with the latest virus definitions. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that it has loaded a new virus definition file, it reports this status.

Table 2-202 Description of the **Virus Definitions are Current** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	Virus Definitions are Current
Rule Name	Virus_Definitions_are_Current
Severity	Notice
Event IDs	16
Description	Detects that the installed virus definitions are current. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the definitions are current, it reports this status.

Table 2-203 Description of the **AntiVirus Realtime Protection Disabled** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Realtime Protection Disabled
Rule Name	AntiVirus_Realtime_Protection_Disabled
Severity	Critical
Event IDs	24

Table 2-203 Description of the **AntiVirus Realtime Protection Disabled** parameters used *(continued)*

Parameter	Description
Description	Detects the disabling of the Symantec AntiVirus real-time system protection option. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the real-time protection option has been disabled, it reports this status.

Table 2-204 Description of the **Virus Detected - Cleaned Failed** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	Virus Detected - Cleaned Failed
Rule Name	Virus_Detected_Cleaned_Failed
Severity	Critical
Event IDs	5, 46, 51
Description	Detects the discovery of a virus or Trojan horse by Symantec AntiVirus. This detection indicates that malicious software has arrived at the client side by email, download, document macro, or by disk-to-disk transfer. This event indicates Symantec AntiVirus client was unable to clean, remove, or quarantine the identified malware and the risk is still present on the system. Immediate investigation is required.

Symantec Endpoint Protection Client Communication

This portion of the policy detects alerts from Symantec Endpoint Protection client installations. This policy can be applied to all Windows hosts with Symantec Endpoint Protection client installations.

Note: This policy auto-detects if the client is running either Symantec Endpoint Protection or previous versions of Symantec AntiVirus.

Table 2-205 Description of the parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	Virus Detected
Rule Name	Virus_Detection
Severity	Critical
Event IDs	5, 46, 51
Description	Detects the discovery of a virus or Trojan horse by Symantec Endpoint Protection. This detection indicates that malicious software has arrived at the client side by email, download, document macro, or by disk-to-disk transfer. Immediate action is usually warranted.

Table 2-206 Description of the **AntiVirus Service Stopped** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Service Stopped
Rule Name	Antivirus_Service_Stopped
Severity	Warning
Event IDs	13
Description	Detects the stopping of the Symantec Endpoint Protection service. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the Symantec AntiVirus service has stopped, it reports this status.

Table 2-207 Description of the **AntiVirus Service Started** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Service Started

Table 2-207 Description of the **AntiVirus Service Started** parameters used *(continued)*

Parameter	Description
Rule Name	Antivirus_Service_Started
Severity	Notice
Event IDs	14
Description	Detects the starting of the Symantec Endpoint Protection service. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the Symantec AntiVirus service has started, it reports this status.

Table 2-208 Description of the **AntiVirus Scan Started** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Scan Started
Rule Name	AntiVirus_Scan_Started
Severity	Notice
Event IDs	3
Description	Detects the starting of a manual scan of a host with Symantec Endpoint Protection. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that it has initiated a manual scan of the host, it reports this status.

Table 2-209 Description of the **AntiVirus Scan Canceled** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Scan Canceled
Rule Name	AntiVirus_Scan_Canceled
Severity	Warning

Table 2-209 Description of the **AntiVirus Scan Canceled** parameters used *(continued)*

Parameter	Description
Event IDs	21
Description	Detects the canceling of a manual scan of a host with Symantec Endpoint Protection. Symantec Endpoint Protection issues the status messages for various application conditions. When Symantec Endpoint Protection determines that it has been commanded to cancel a manual scan, it reports this status.

Table 2-210 Description of the **AntiVirus Scan Completed** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Scan Completed
Rule Name	AntiVirus_Scan_Completed
Severity	Warning
Event IDs	2
Description	Detects the completion of a manual scan of a host with Symantec Endpoint Protection. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that it has successfully completed a manual scan, it reports this status.

Table 2-211 Description of the **New Virus Definition Loaded** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	New Virus Definition Loaded
Rule Name	New_Virus_Defintion_Loaded
Severity	Notice
Event IDs	7

Table 2-211 Description of the **New Virus Definition Loaded** parameters used *(continued)*

Parameter	Description
Description	Detects the updating of Symantec Endpoint Protection with the latest virus definitions. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that it has loaded a new virus definition file, it reports this status.

Table 2-212 Description of the **Virus Definitions are Current** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	Virus Definitions are Current
Rule Name	Virus_Definitions_are_Current
Severity	Notice
Event IDs	16
Description	Detects that the installed virus definitions are current. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the definitions are current, it reports this status.

Table 2-213 Description of the **AntiVirus Realtime Protection Disabled** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	AntiVirus Realtime Protection Disabled
Rule Name	AntiVirus_Realtime_Protection_Disabled
Severity	Critical
Event IDs	24

Table 2-213 Description of the **AntiVirus Realtime Protection Disabled** parameters used *(continued)*

Parameter	Description
Description	Detects the disabling of the Symantec Endpoint Protection real-time system protection option. Symantec Endpoint Protection issues the status messages for various application conditions and errors. When Symantec Endpoint Protection determines that the real-time protection option has been disabled, it reports this status.

Table 2-214 Description of the **Virus Detected - Cleaned Failed** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus Client Communication
Option	Virus Detected - Cleaned Failed
Rule Name	Virus_Detected_Cleaned_Failed
Severity	Critical
Event IDs	5, 46, 51
Description	Detects the discovery of a virus or Trojan horse by Symantec Endpoint Protection. This detection indicates that malicious software has arrived at the client side by email, download, document macro, or by disk-to-disk transfer. This event indicates that the Symantec Endpoint Protection client was unable to clean, remove, or quarantine the identified malware. It also indicates that the risk is still present on the system. Immediate investigation is required.

System External Device Activity

This option group subsection monitors for specific external device activity such as the various activities that are associated with USB devices and CD and DVD burning. This activity should be monitored on an enterprise network, as such devices may pose the threat of data loss.

USB Device Activity

This portion of the policy detects activity that is associated with USB devices.

Table 2-215 Description of the **USB Registry Connect Activity** parameters used

Parameter	Description
Option Path	System External Device Activity > USB Device Activity
Option	USB Registry Connect Activity
Rule Name	USB_Registry_Connect_Activity
Severity	Warning
Noise Suppress	1 Minute. Suppress reporting of events from this rule for specified duration after the rule has triggered once.
Registry Paths	\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\ENUM\USB\*
Description	Detects the USB device connection activity that is associated with the Windows registry. This rule provides a noise suppression duration value to tune out the unnecessary noise that this rule may cause.

CD/DVD Burning Activity

This portion of the policy detects the various activities that are associated with CD and DVD burning.

Note: These rules function only in Windows 2000/2003 environments.

Table 2-216 Description of the **CD/DVD Burning Services** parameters used

Parameter	Description
Option Path	System External Device Activity > CD/DVD Burning Activity
Option	CD/DVD Burning Services Enabled
Rule Name	CD_DVD_Burning_Activity_Enabled
Severity	Warning
Event IDs	7040
Description	Detects a CD/DVD service auto start configuration event from the Windows Event Log.

Table 2-217 Description of the **CD/DVD Burning Services Enabled** parameters used

Parameter	Description
Option Path	System External Device Activity > CD/DVD Burning Activity
Option	CD/DVD Burning Services Enabled
Rule Name	CD_DVD_Burning_Activity_Enabled
Severity	Warning
Event IDs	7036
Description	Detects when the CD/DVD service enters a running state from the Windows Event Log.

Table 2-218 Description of the **CD/DVD Burning Services Stopped** parameters used

Parameter	Description
Option Path	System External Device Activity > CD/DVD Burning Activity
Option	CD/DVD Burning Services Stopped
Rule Name	CD_DVD_Burning_Activity_Stopped
Severity	Warning
Event IDs	7035
Description	Detects when the CD/DVD service enters a stopped state from the Windows Event Log.

System Attack Detection

This option group subsection contains basic Web attack monitoring criteria to thwart basic attacks on any Web server that produces any kind of access log.

Note: The access log must follow W3C guidelines. The majority of Web server applications on Windows servers are Internet Information Services (IIS). By default, System Attack Detection is set up for IIS. You can set up this area for any Web hosting application. Within this option group subsection there is a global settings area to set several unique properties for the rest of the system attack monitor.

The global settings area consists of the following:

- Alert only on Success Attack Attempt (Code 200): This area configures all the attack detection rules to look for the trailing code 200 when a suspicious string is found in the access log. Trailing code 200 means a successful process request. This setting dramatically decreases the amount of false positives and provides administrators with events that are considered processed by the hosting system.
- Web Access Log File Path: This area configures the Web access log path, which the rules in this policy subsection sift through to find malicious request strings. Symantec Critical System Protection provides a default IIS 7 location.
- Whitelisted IP Addresses: This area configures the IP addresses that are allowed or otherwise ignored in this monitoring subsection. These IP addresses are for tools like automated vulnerability scanning systems on enterprise networks, where you know that at regular intervals Web attack tests occur.
- Blacklisted IP Addresses: This area configures the IP addresses that are not allowed access to the host system. Blacklisted IP addresses may be any addresses outside an internal network range if this area monitored an intranet Web host. Blacklisted IP addresses may also be known bad IP addresses from any of the blacklists available on the Internet.
- IIS HTTP Success Code: The IIS HTTP Success Code is the trailing HTTP code on all requests that signifies that the request has been successfully processed on the host Web system. A success code that is paired with a maliciously crafted URI string would indicate a possible compromised system.
- IIS HTTP Error Code: The IIS HTTP Error Code is the HTTP error code that signifies a bad HTTP request. A high frequency repeating number of these found in the access log signifies that a possible Web vulnerability scan is occurring.

Generic Web Attack Detection Monitoring

Table 2-219 Description of the **Generic VA scan Attempt** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic VA scan Attempt
Rule Name	WebAttackDetection_Generic_VAScan
Severity	Warning

Table 2-219 Description of the **Generic VA scan Attempt** parameters used *(continued)*

Parameter	Description
Invalid Count	20 Times in which a 404 or unknown request is received.
Interval	2 minutes Time frequency in which invalid count needs to occur to trigger event.
Description	Detects a possible VA scan by triggering an event within a specific administrator-defined threshold. If Symantec Critical System Protection receives a specified number of 404 error codes by a user-defined frequency, then this rule generates an alert on a possible VA scan attempt.

Table 2-220 Description of the **Generic Blacklisted IP Request Attempts** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic Blacklisted IP Request Attempts
Rule Name	WebAttackDetection_Generic_BlackListedIP
Severity	Warning
Description	A simple rule that detects the access attempt by a blacklisted IP address that is found in the HTTP access log. You configure the blacklisted IP address in the Global Settings area. If you enable this rule, any attempt by the predefined blacklisted IP address generates an event.

Table 2-221 Description of the **Generic SQL Injection Attack Attempts** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic SQL Injection Attack Attempts
Rule Name	WebAttackDetection_Generic_SQLInjection
Severity	Warning

Table 2-221 Description of the **Generic SQL Injection Attack Attempts** parameters used *(continued)*

Parameter	Description
Description	Detects the very simple and generic SQL injection-type attacks when it monitors the HTTP access log file. Primary and secondary select logic is used to ensure that accurate rule tuning can occur. You can customize this area to your needs to add further SQL injection measures.

Table 2-222 Description of the **Generic Directory Transversal Attempts** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic Directory Transversal Attempts
Rule Name	WebAttackDetection_Generic_DirTransversal
Severity	Warning
Description	Detects possible directory transversal attempts in HTTP request strings. The generic strings for directory transversal attempts are provided. An individual or script attempting to transverse directories by HTTP request may be considered a malicious action.

Table 2-223 Description of the **Generic Malicious User Agent Request Attempts** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic Malicious User Agent Request Attempts
Rule Name	WebAttackDetection_Generic_MaliciousUserAgent
Severity	Warning
Description	Detects the malicious user agent strings in HTTP requests. Automated scripts commonly use bad user agents in large-scale attacks. Pre-scripted suites of programs also use them to attack a Web server. The presence of these known-bad user agent strings may indicate a malicious attempt to access your host Web system.

Table 2-224 Description of the **Generic Unwanted Extension Requests** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic Unwanted Extension Requests
Rule Name	WebAttackDetection_Unwanted_Extension_Request
Severity	Warning
Description	Detects the unwanted or suspicious extension requests. Files that are requested with the extensions configured in this rule may indicate a malicious script or user. You can add or remove extensions in this area to customize this event per host system environment.

Table 2-225 Description of the **Generic Unwanted Directory Requests** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic Unwanted Directory Requests
Rule Name	WebAttackDetection_Unwanted_Directory_Request
Severity	Warning
Description	Detects the unwanted or suspicious directory requests. Directory requests as configured in this rule may indicate a malicious script or user. You can add or remove sensitive directory paths in this area to customize this event per host system environment.

Table 2-226 Description of the **Generic Vulnerable CGI Requests** parameters used

Parameter	Description
Option Path	System Web Attack Detection Monitor > Generic VA Scan Attempt
Option	Generic Vulnerable CGI Requests
Rule Name	WebAttackDetection_Generic_VulnerableCGIRequest
Severity	Warning

Table 2-226 Description of the **Generic Vulnerable CGI Requests** parameters used *(continued)*

Parameter	Description
Description	Detects the unwanted or suspicious CGI and script requests. CGI and script requests as configured in this rule may indicate a malicious script or user. You can add or remove sensitive directory paths in this area to customize this event per host system environment.