Symantec™ Event Collector 4.3 for Microsoft® Internet Information Services (IIS) Quick Reference

Symantec™ Event Collector for Microsoft® Internet Information Services (IIS) Quick Reference

Legal Notice

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA

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 feature and function, installation, and configuration. The Technical Support group also authors 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
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade insurance and maintenance contracts
- Information about the Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support

Chapter 1 Introducing Symantec Event Collector for Microsoft Internet Information Services (IIS)

About this quick reference 9
Compatibility requirements 10
Compatibility requirements for the event collector 10
System requirements for the collector computer 10
Preinstallation requirements for Microsoft IIS Event Collector 10
Configuring your security product to work with the collector 11
Configuring Microsoft IIS to work with the collector 11
About the installation sequence for Microsoft IIS Event Collector 11
Sensor configuration for Microsoft IIS Event Collector 12
Sensor settings for Microsoft IIS Event Collector 12

Chapter 2 Implementation notes

Implementation notes for Microsoft IIS Event Collector 15
Product ID 15
Method of data collection 15
Schema packages 15
Example data 15
Event mapping for Information Manager 16

Chapter 3 Event filtering and aggregation

Event filtering and aggregation for Microsoft IIS Event Collector 23

Index

Chapter 1

Introducing Symantec Event Collector for Microsoft Internet Information Services (IIS)

This chapter includes the following topics:

- About this quick reference
- Compatibility requirements
- Preinstallation requirements for Microsoft IIS Event Collector
- Configuring your security product to work with the collector
- About the installation sequence for Microsoft IIS Event Collector
- Sensor configuration for Microsoft IIS Event Collector

About this quick reference

This quick reference includes information that is specific to Symantec Event Collector for Microsoft Internet Information Services (IIS). General knowledge on installing and configuring collectors is assumed, as well as basic knowledge of Microsoft IIS.

For detailed information on how to install and configure event collectors, please see the *Symantec Event Collectors Integration Guide*.

For information on Microsoft IIS, see your product documentation.

Compatibility requirements

The collector is compatible with specific versions of the security product and is compatible with certain operating systems.

Compatibility requirements for the event collector

The collector is compatible with Microsoft Internet Information Services (IIS) versions 5.x and 6.x.

The collector runs on the following operating systems:

- Microsoft Windows 2000 with Service Pack 4 or later
- Microsoft Windows 2000 Advanced Server with Service Pack 4 or later
- Microsoft Windows 2003 Server Enterprise Edition with Service Pack 1 or later
- Microsoft Windows 2003 Server Standard Edition with Service Pack 1 or later
- Microsoft Windows XP with Service Pack 2 or later

System requirements for the collector computer

The computer on which you install the collector must meet the following minimum system requirements:

- Intel Pentium-compatible 133-MHz processor (up to and including Xeon-class)
- 512 MB minimum, 1 GB of memory recommended for the Symantec Event Agent
- 35 MB of hard disk space for collector program files
- 95 MB of hard disk space to accommodate the Symantec Event Agent, the JRE, and the collector
- TCP/IP connection to a network with a fixed IP address

Preinstallation requirements for Microsoft IIS Event Collector

The collector does not have preinstallation requirements.

Configuring your security product to work with the collector

After you install the necessary collector components, you must configure Microsoft IIS so that the event information is available to the collector.

For detailed information on configuring Microsoft IIS, see your security product documentation.

Configuring Microsoft IIS to work with the collector

You can use the configuration tools that are provided with Microsoft IIS to configure Microsoft IIS. You must configure Microsoft IIS to log with a W3C-log format with all fields enabled to be logged.

To configure Microsoft IIS

1. From the Microsoft Internet Information Server menu, start Internet Service Manager.
2. Double-click the local computer.
3. Double-click the Web Sites or FTP Sites folder, right-click the Web site or FTP site for which you want to enable logging, and then click **Properties**.
4. On the Web Site, FTP Site, or General tab (depending on which type of site you are configuring), check **Enable logging**.
5. In the Active log format box, click **W3C Extended Log File Format**.
6. Click **Properties**.
7. In the Extended Logging Properties page, on the Extended Logging Options tab, check all of the boxes.
8. Click **OK**.
9. Click **Apply**, and then click **OK**.

About the installation sequence for Microsoft IIS Event Collector

The collector installation sequence is as follows:

- Close the Symantec Security Information Manager Client console.
- Register the collector.
- Install the Symantec Event Agent.

Symantec Event Agent build 12 or later is required.

- Install the collector component.

For more information, see the *Symantec Event Collectors Integration Guide*.

Sensor configuration for Microsoft IIS Event Collector

The collector uses a sensor that you must configure to receive security events. After you configure the sensor, distribute the settings to the collectors on the target computers.

For more information, see the *Symantec Event Collectors Integration Guide*.

Sensor settings for Microsoft IIS Event Collector

The collector uses a log file sensor.

The collector includes two default sensor configurations: one reads HTTP logs and the other reads FTP logs.

The sensor has the following properties:

- Log file directory
  Specify the path to the log file on the security product computer.
  For the HTTP log, the default log file directory is C:\\winnt\system32\LogFiles\W3SVC1
  For the FTP log, the default log file directory is C:\\winnt\system32\LogFiles\MSFTPSVC1
  See "Configuring your security product to work with the collector" on page 11.
- Log File Name
  Specify the name of the log file.
  For both the HTTP log and the FTP log, the default log file extension is .log.
  An example log file name is exyymmdd.log.
- Reading Mode
  Specify whether the collector checks for new log files after reaching the end of the current log file or waits for new events to be added to the current log file.
  Specify Monitor Dynamic Log for the collector to check for a new log file to read.
- Start Reading From
  Specify End to read the log file from the end of the file upon the restart of the collector.
  End is the default value for both HTTP logs and FTP logs.

Specify Last Position for the collector to keep track of which line the collector is reading in the log file. If the collector is interrupted and restarted, reading continues from this position. When the collector is started for the first time, the collector reads all events in all files.

Chapter 2

Implementation notes

This chapter includes the following topics:

- Implementation notes for Microsoft IIS Event Collector

Implementation notes for Microsoft IIS Event Collector

This section describes the implementation details for the Microsoft IIS Event Collector.

Product ID

The product ID for the collector is 3149.

Method of data collection

The collector uses a LogFile sensor to collect events.

Schema packages

The collector uses the following schema packages:

- IDS events
- Firewall events

Example data

Example data is as follows:

```
W3C - 2006-01-20 05:37:37 10.194.63.10 - W3SVC1 SHIRE
10.194.63.11 80 GET /iisstart.asp - 200 0 0 593 719 HTTP/1.1
```

```
10.194.63.11 ELinks+(0.4.2;+Linux;+104x54) - http://10.194.63.11/

NCSA - 10.194.63.10 - - [20/Jan/2006:00:38:07 -0500] "GET
/iisstart.asp HTTP/1.1" 200 0

MS IIS - 10.194.63.10, -, 1/20/2006, 0:38:27, W3SVC1, SHIRE,
10.194.63.11, 0, 593, 0, 200, 0, GET, /iisstart.asp, -,

FTP W3C - 2006-01-20 03:26:34 10.194.63.10 administrator MSFTPSVC1
SHIRE 10.194.63.11 21 [5]created iis-test.log - 226 0 0 675 16
FTP - - - -
```

Event mapping for Information Manager

Table 2-1 shows the Information Manager field name and comments.

Table 2-1 Event mapping

Information Manager field name	Microsoft IIS Event Collector field name	Comment
Category ID	N/A	Actual value (30007606 - Security)
Description	N/A	Description of the event
Destination Host Name	N/A	Destination host name
Destination Service Name	N/A	Application protocol that is used for the connection A common value is HTTP.
Event Code	N/A	Depends on the target operation: If the target operation is a GET event code then the value is 10641. If the target operation is a PUT event code then the value is 4456.
Event Date	N/A	Date of the event
Event Details	N/A	517200 - No additional details
Event Info 1	N/A	HTTP result code

Table 2-1 Event mapping *(continued)*

Information Manager field name	Microsoft IIS Event Collector field name	Comment
Event Info 2	N/A	Bytes sent
Event Info 3	N/A	Bytes received
Event Type ID	N/A	Possible values: 1032000 - Host Intrusion Event 1732000 - Generic Firewall 512000 - Connection Accepted 512001 - Connection Rejected
Intrusion Action	N/A	Attempted action Possible values: 1037213 - Login 1037203 - Create 1037204 - Access 1037208 - Move 1037206 - Delete 1037214 - Logout
Intrusion Data	N/A	String that contains additional data that is specific to this event
Intrusion Intent	N/A	Overall intent of the attempted intrusion activity Possible values: 1027103 - Access 1027104 - Integrity
Intrusion Outcome	N/A	Possible values: 1027202 - Unknown 1027203 - Succeeded 1027204 - Failed
Intrusion Source Process	N/A	Individual session or process identifier for FTP

Table 2-1 Event mapping *(continued)*

Information Manager field name	Microsoft IIS Event Collector field name	Comment
Intrusion Target Name	N/A	Name of the attacker's target
Intrusion Target Type	N/A	Type of the attacker's target Possible values: 1037112 - User Account 1037105 - File 1037106 - Directory
IP Destination Address	N/A	IP address of the Web server
IP Destination Port	N/A	IP destination port
IP Source Address	N/A	IP source address
IP Source Port	N/A	IP address source port
Severity ID	N/A	See Table 2-2
Source Host Name	N/A	Source host name

Table 2-1 Event mapping *(continued)*

Information Manager field name	Microsoft IIS Event Collector field name	Comment
Target Operation	N/A	HTTP command Possible values: GET PUT HEAD MKDIR RMDIR DELETE OPTIONS PROPFIND INDEX FTP command Possible values: PASS CREATED SENT RNFR RNTO USER MKD DELE QUIT
Target Resource	N/A	URL that is being requested
User ID	N/A	ID that is used for operations that require user authentication
User Name	N/A	Client-side user name where available
Vendor Device ID	N/A	62

Table 2-1 Event mapping *(continued)*

Information Manager field name	Microsoft IIS Event Collector field name	Comment
Vendor Signature	N/A	Vendor description of current operation

Table 2-2 shows severity mapping.

Table 2-2 Severity mapping

Vendor Signature	Severity
Default value	1 - Informational
For result code - 230	2 - Warning

Table 2-2 Severity mapping *(continued)*

Vendor Signature	Severity
Severity depends on the vendor signature value	3 - Minor
Possible values:	
IISCGIphf	
IISWWWBoardPassword	
IISCGIWrap	
IISCGIWhoisraw	
IISCGIWebsendmail	
IISCGIWebplusabout	
IISCGIWebgais	
IISCGIWebcart	
IISCGIViewsource	
IISCGITestCGI	
IISCGISojourn	
IISCGISiteusermod	
IISCGIShell	
IISCGIBatPipe	
IISCGIPrintenv	
IISCGIPlusmail	
IISCGIPfdispaly	
IISCGIPerl	
IISHTTPconfigsys	
IISASPSourceDisclosure	
IISCGIjj	
IISCGIinfosrch	
IISCGIinfo2www	

Table 2-2 Severity mapping *(continued)*

Vendor Signature	Severity
IISHTTPidqDirTraversal IISCGIIcat IISCGIhtmlscript IISCGIhtsearch IISCGIguestbook IISCGIaglimpse IISCGIfinger IISCGIfaxsurvey IISCGIloadpage IISCGIarchitextquery IISCGIdumpenv IISCGIcampas IISCGIcachemgr IISCGIbbhist IISCGIalibaba IISCGIget32 IISCGIformhandler IISCGIwebdist IISCGIWebspeedAdmin IISCGIWebdriver IISCGIWebcomguestbook IISCGIAnyform IISCGIBnbform IISCGIFilespl	3 - Minor (continued)
The severity depends on the vendor signature value. Possible values: IISDotDotAttack IISCrossSite	4 - Major

Chapter 3

Event filtering and aggregation

This chapter includes the following topics:

- Event filtering and aggregation for Microsoft IIS Event Collector

Event filtering and aggregation for Microsoft IIS Event Collector

Table 3-1 shows the default filters available with the collector. All filters are disabled by default.

Table 3-1 Default filters

Filter Name	Criteria	Description
Remove not translated events	Remove events where the field not_translated is equal to true.	This filter removes all events or log file rows that were not translated (useless events).
Filter non-identified	Remove events where the field not_identified contains the value NotIdentified.	This filter removes all requests that have not been identified as malicious. It is enabled when the collector is in an IDS mode of operation. This filter is not enabled but should be enabled in most cases to minimize the sending of events which are of little value.

Table 3-1 Default filters *(continued)*

Filter Name	Criteria	Description
Filter File Not Found	Remove events with an HTTP result code of 404.	This filter removes all events where the requested page did not exist. These requests are usually noise traffic and not a security risk. This filter is not enabled but should be enabled in most cases to minimize the sending of events which are of little value.
Filter Successful	Remove events with an HTTP result code of 200.	This filter removes all events where the requested page existed and the client was able to retrieve it. These events are high-risk if the request is malicious.
Filter Forbidden	Remove events with an HTTP result code of 403.	This filter removes all events where the client was forbidden from viewing the page that is requested. These events are high-risk because the client may be attempting to view restricted data.
Filter Error	Remove events with an HTTP result code of 500.	This filter removes all events where the client request resulted in an error on the server. These events are high-risk as the arguments or actions of the client may be malicious with the errors being a side effect.

Because of the role that intrusion-detection point products such as Microsoft IIS play in defense-in-depth scenarios, filtering or aggregation on these types of events is not recommended. However, it is possible that systems on a network play a specific role to ensure the security of an organization. This type of role may result in false positives from the device. For example, computers within the network that are responsible for assessing vulnerability risks may use techniques that cause intrusion-detection point products to report that the network is under attack. If you have this type of scenario, you may consider aggregating the events from that computer. This aggregation is based on the IP Source Address value in the Common Event folder.

You may also consider securing the network by aggregating or filtering events from this computer that are consistently fired by the role the computer plays on the network. This aggregation is based on the vendor code of the events you want to filter.

Index

C

compatibility requirements 10
configuring
    Microsoft IIS 11
    sensor 12

I

implementation notes 15
installation 11

M

mapping 15
Microsoft IIS configuration 11

P

preinstallation requirements 10

R

requirements
    compatibility 10
    preinstallation 10
    system 10

S

sensor configuration 12
system requirements 10