Symantec™ Security Information Manager 4.7.4 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 4.7.4

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo 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.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

■ A range of support options that give you the flexibility to select the right amount of service for any size organization
■ Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
■ Upgrade assurance that delivers software upgrades
■ Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
■ Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

Licensing and registration
If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:
www.symantec.com/business/support/

Customer service
Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:
  - Questions regarding product licensing or serialization
  - Product registration updates, such as address or name changes
  - General product information (features, language availability, local dealers)
  - Latest information about product updates and upgrades
  - Information about upgrade assurance and support contracts
  - Information about the Symantec Buying Programs
  - Advice about Symantec's technical support options
  - Nontechnical presales questions
  - Issues that are related to CD-ROMs 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
Chapter 1 Overview ................................................................. 9
  Documentation .......................................................................... 9
  About Symantec Security Information Manager ..................... 10

Chapter 2 What's new in Symantec Security Information Manager 4.7.4 .......................................................... 13
  Symantec SIEM 9700 Series appliances ........................................ 13
  Role-based access to the Event Query Templates ....................... 14
  SSIM Web Start Client .............................................................. 14
  Navigation option for Event Storage Rules list ......................... 14

Chapter 3 SSIM Web Start Client ................................................. 15
  About SSIM Web Start Client ..................................................... 15
  Launching the SSIM Web Start Client ....................................... 15
    Enabling ActiveX controls and plug-ins to launch SSIM Web Start
    Client ............................................................................... 17
    Enabling JavaScript to launch SSIM Web Start Client ............. 17
    Adding a Web site as a trusted site to launch SSIM Web Start
    Client ............................................................................... 18
  Third-party certificate for SSIM Web Start client ..................... 18
  Uninstalling SSIM Web Start Client ........................................ 19

Chapter 4 Issues ........................................................................ 21
  Resolved issues ........................................................................ 21
  Known issues ........................................................................... 22
Overview

This chapter includes the following topics:

- Documentation
- About Symantec Security Information Manager

Documentation

The following documentation is available for Information Manager:

- **Help for the Web configuration interface and the Information Manager console (client)**
  - Contains the information on how to use the product. You can access Help by clicking the Help icon in any dialog box, or by pressing the F1 key.

- **Symantec Security Information Manager User Guide**
  - Contains the information on how to use the product.
  - The document is in PDF format.

- **Symantec Security Information Manager Administrator Guide**
  - Contains the information on how to manage the configuration and administrative tasks after the installation.
  - The document is in PDF format.

- **Symantec Security Information Manager Installation Guide**
  - Contains the information on how to install and upgrade the product.
  - The document is in PDF format.

- **Symantec Security Information Manager Reporting Guide**
  - Contains the information on how to use the reporting feature in the product.
  - The document is in PDF format.
About Symantec Security Information Manager

Information Manager provides real-time event correlation and data archiving to protect against security threats and to preserve critical security data. Information Manager collects and archives security events from across the enterprise. These events are correlated with the known asset vulnerabilities and current security information from the Global Intelligence Network. The resulting information provides the basis for real-time threat analysis and security incident identification. Information Manager archives the security data for forensic and regulatory compliance purposes.

Information Manager collects, analyzes, and archives information from security devices, critical applications, and services, such as the following:

- Firewalls
- Routers, switches, and VPNs
- Enterprise antivirus
- Intrusion detection systems and Intrusion Prevention Systems
- Vulnerability scanners
- Authentication servers
- Windows and UNIX system logs

Information Manager provides the following features to help you recognize and respond to threats in your enterprise:

- Normalization and correlation of events from multiple vendors.
- Event archives to retain events in both their original (raw) and normalized formats.
- Distributed event filtering and aggregation to ensure that only relevant security events are correlated.
- Real-time security intelligence updates from Global Intelligence Network. These updates keep you apprised of global threats and let you correlate internal security activity with external threats.
- Customizable event correlation rules to let you fine-tune threat recognition and incident creation for your environment.

- Security incident creation, ticketing, tracking, and remediation for quick response to security threats. Information Manager prioritizes incidents based upon the security policies that are associated with the affected assets.

- An Event Viewer that lets you easily mine large amounts of event data and identify the computers and users that are associated with each event.

- A client-based console from which you can view all security incidents and drill down to the related event details. These details include affected targets, associated vulnerabilities, and recommended corrective actions.

- Predefined and customizable queries to help you demonstrate compliance with the security and the data retention policies in your enterprise.

- A Web-based configuration interface that lets you view and customize the dashboard, configure settings, and manage events, incidents, and tickets remotely. You can download various utilities and perform routine maintenance tasks such as backup and restore. You can use the custom logs feature with the universal collectors to collect and map information from devices for which standard collectors are not available.
Overview

About Symantec Security Information Manager
What's new in Symantec Security Information Manager 4.7.4

This chapter includes the following topics:

■ Symantec SIEM 9700 Series appliances
■ Role-based access to the Event Query Templates
■ SSIM Web Start Client
■ Navigation option for Event Storage Rules list

Symantec SIEM 9700 Series appliances

Symantec SIEM 9700 Series appliances are scalable security information and event management appliances. These appliances provide reliable performance with Information Manager software. The SIEM 9700 Series is comprised of three models; the 9750, the 9751, and the 9752. Each model provides 3.9TB of redundant event storage and dedicated Remote Management Module features to allow remote management of the appliance. In addition, the 9751 and 9752 provide enterprise connectivity through 8GB Fibre Channel. Each physical appliance can be combined seamlessly with virtual appliances to ease interoperability.

For more information, see the following guides:

■ Symantec SIEM 9700 Series Appliances Maintenance Guide
■ Symantec SIEM 9700 Series Appliances Installation Guide
■ Symantec SIEM 9700 Series Appliances Product Description Guide
Role-based access to the Event Query Templates

In Information Manager, an administrator can restrict the access of a user to Event Query Templates. Access to Event Query Templates can be controlled based on the View Event Query Templates permission that is granted to a role. By default, this permission is enabled for new roles.

If the View Event Query Templates permission is disabled for a role, the user who is assigned with this role cannot access the Templates folder on the Events view. If the View Event Query Templates permission is enabled for a role, the user who is assigned with this role can access and run the Event Query Templates.

SSIM Web Start Client

By using SSIM Web Start Client, you can now reach the Information Manager console directly without downloading and installing the Information Manager console.

The Launch SSIM Web Start Client link, that is located on the logon page of the Information Manager Web configuration interface, launches the Information Manager console. You can also access this link from the Downloads option on the Home view of the Web configuration interface.

See “Launching the SSIM Web Start Client” on page 15.

Navigation option for Event Storage Rules list

A Move to top option and a Move to bottom option are now available in the Event Storage rules list. These options can be used to move a rule directly to the top or to the bottom of the list.
SSIM Web Start Client

This chapter includes the following topics:

- About SSIM Web Start Client
- Launching the SSIM Web Start Client
- Third-party certificate for SSIM Web Start client
- Uninstalling SSIM Web Start Client

About SSIM Web Start Client

By using SSIM Web Start Client, you can now reach the Information Manager console directly without downloading and installing the Information Manager console.

The Launch SSIM Web Start Client link, that is located on the logon page of the Information Manager Web configuration interface, launches the Information Manager console. You can also access this link from the Downloads option on the Home view of the Web configuration interface. When the Information Manager console is launched for the first time, a shortcut icon is created for SSIM Web Start Client on the Windows® Desktop and Start menu. Later, this shortcut icon can be used for launching the Information Manager console.

See “Launching the SSIM Web Start Client” on page 15.

Launching the SSIM Web Start Client

You can launch the SSIM Web Start Client from the Information Manager Web configuration interface using the Launch SSIM Web Start Client link on the logon page.
When you launch the SSIM Web Start Client for the first time, the files that are required are downloaded to the client computer and the Information Manager logon dialog box appears. A shortcut icon is created for SSIM Web Start Client on the Windows® Desktop and Start menu.

See “SSIM Web Start Client” on page 14.

The minimum version of JRE that is required for the SSIM Web Start Client is 1.6.0_19. The recommended version is 1.6.0_26. For the SSIM Web Start Client to work correctly, with 64-bit Java installed, you must use a 64-bit browser. With 32-bit Java installed, you must use a 32-bit browser.

The appropriate Java version must be installed on the computer. After Java is installed, you must also enable the ActiveX controls and plug-ins from Internet Explorer.

See “Enabling ActiveX controls and plug-ins to launch SSIM Web Start Client” on page 17.

Make sure to enable JavaScript for the browser that is used for launching SSIM Web Start Client.

See “Enabling JavaScript to launch SSIM Web Start Client” on page 17.

An error message may be displayed if the Web site that launches SSIM Web Start Client is not added to the list of trusted sites.

See “Adding a Web site as a trusted site to launch SSIM Web Start Client” on page 18.

Note: The console that is launched by SSIM Web Start Client is not FIPS-compliant. If you require a FIPS-compliant console, you must download and run Setup.exe from the Install SSIM Client link on the logon page of the Information Manager Web configuration interface.

To launch the SSIM Web Start Client

1 In the browser, type https:// followed by the address of the Information Manager server and then press Enter.

2 Click Launch SSIM Web Start Client link.

You can also access this link from the Downloads option on the Home view of the Web configuration interface.
3 In the **Warning - Security** dialog box, click **Yes** to continue.

   If the Information Manager server is added as a trusted site, this warning does not appear.

   The files that are required to launch SSIM Web Start Client are downloaded and then the logon page of the Information Manager console appears.

4 Enter the appropriate credentials to log on to Information Manager.

---

**Note:** When you log on to the SSIM Web Start Client, the JRE version that is displayed in the **Help > About Symantec Security Information Manager** dialog box is the version of the JRE that is installed on the client computer. The Client JRE version may be different than the JRE version that is installed on the Information Manager server.

### Enabling ActiveX controls and plug-ins to launch SSIM Web Start Client

Java must be installed on the computer that launches SSIM Web Start Client. After Java is installed, make sure to enable the ActiveX controls and plug-ins from Internet Explorer.

**To enable ActiveX and plug-ins**

1. From Internet Explorer, go to **Tools > Internet Options**.
2. From the **Security** tab, select **Trusted Sites** and then click **Custom Level**.
3. Scroll down to **ActiveX Controls and plug-ins > Run ActiveX Controls and plug-ins**.
4. Check **Enable**.

   See “Launching the SSIM Web Start Client” on page 15.

### Enabling JavaScript to launch SSIM Web Start Client

JavaScript must be enabled for the browser that is used for launching SSIM Web Start Client.

**To enable JavaScript for computers with Internet Explorer 7/8**

1. From Internet Explorer, go to **Tools > Internet Options**.
2. From the **Security** tab, select **Trusted Sites**, and then click **Custom Level**.
3. Scroll down to **Scripting > Active scripting** and check **Enable**.
4. Click **OK**.
5. Click **Yes** in the warning dialog box and then click **OK**.
To enable JavaScript for computers with Firefox 3.6/4.0

1. Open Firefox, click Tools, and then select Options.
2. From the Content tab, check Enable JavaScript.
3. Click OK.

See “Adding a Web site as a trusted site to launch SSIM Web Start Client” on page 18.

See “Launching the SSIM Web Start Client” on page 15.

Adding a Web site as a trusted site to launch SSIM Web Start Client

When SSIM Web Start Client is launched by using Internet Explorer 7/8 and if the Web site that is used for launching SSIM Web Start Client is not added as a trusted site, an error may be displayed. To resolve this error, you must add the Web site as a trusted site.

To add a Web site as a trusted site to launch SSIM Web Start Client

1. Open Internet Explorer 7/8, go to Tools > Internet Options.
2. From the Security tab, select Trusted Sites, and then click Sites.
3. Type https:// followed by the URL of the Fully Qualified Domain Name (FQDN) or the IP address of the Web site.
4. Click Add

See “Launching the SSIM Web Start Client” on page 15.

Third-party certificate for SSIM Web Start client

With SSIM Web Start client, you can install JRE at any location. It is not bundled with the Information Manager console.

When a third-party certificate is installed on the server, the appropriate certificate must be added on the client side to access the server. The certificate must be placed at the appropriate location, that is, the jre/bin folder of the Java that is used to launch the Information Manager client.

To add the certificate on the client side

1. From the command line, run javaws –viewer
2. Select the Java tab, click View, and verify the path.
3 Place the certificate in Java’s jre\bin folder.

4 Import the certificate using the following command from a command line:

```
keytool.exe -import -file <file_location> -keystore ..\lib\security\cacerts -storepass <certificate_password>
```

*<file_location>* refers to the path and file name of the certificate.

*<certificate_password>* refers to the password created with the certificate.

The Java default certificate password is ‘changeit’.

For example,

```
C:\Program Files\Java\jre6\bin\keytool.exe -import -file C:\Program Files\Java\jre6\bin\cacert.pem -keystore ..\lib\security\cacerts -storepass changeit
```

---

**Uninstalling SSIM Web Start Client**

Symantec recommends to uninstalling SSIM Web Start program from the Java Control Panel. However, you can also uninstall the program from the Windows Control Panel.

---

**Note:** You cannot uninstall SSIM Web Start Client, if the server which is associated with SSIM Web Start Client is unavailable. Before uninstalling SSIM Web Start Client, ensure that this server is available or associate SSIM Web Start Client with the server on which it is currently running. To associate SSIM Web Start Client with a new server, you must launch SSIM Web Start Client from that server.

---

Use the following procedure to uninstall SSIM WebStart Client from Java Control Panel:

**To uninstall SSIM Web Start client from Java Control Panel**

1 On the **Start** menu, click **Run**.

   Make sure that the Information Manager console is closed.

2 Type `javaws -viewer` in the **Run** dialog box and then click **OK** or go to **Start > Control Panel** and then click **Java**.

3 In the **Java Cache Viewer** dialog box, from the list of applications, select **SSIM Web Start Client** and then click the **Remove selected items** icon.

4 From the **General** tab, click **Settings**.

5 In the **Temporary File Settings** dialog box, click **Delete files**.

6 In the **Delete Temporary Files**, dialog box check all the options and then click **OK**.
Use the following procedure to uninstall SSIM Web Start Client from Windows Control Panel:

**To uninstall SSIM Web Start Client**

1. From **Add or Remove Programs** or **Programs and Features**, select **SSIM Web Start Client** and click **Uninstall** or **Remove**.
   
   Make sure that the Information Manager console is closed.

2. Click **Yes** to continue.

3. Click **OK** to confirm and remove SSIM Web Start Client and all of its components.

See “**SSIM Web Start Client**” on page 14.
This chapter includes the following topics:

■ Resolved issues
■ Known issues

Resolved issues

Symantec Security Information Manager 4.7.4 includes the following resolved issues:

■ When the Information Manager restarts during the installation, the default installation option lets you continue the installation from the hard drive after 5 minutes. This option facilitates continuous installation on those computers from which the Installation DVD is not ejected automatically.

■ The My Open Tickets filter is now set as the default filter on the Tickets tile.

■ Previously, if an invalid input was provided when you deploy a rule, the Unable to compile Java error was displayed. This error message has been changed, and an appropriate message is displayed.

■ Previously, the main Incidents page was not viewable when the focus is on the Logs tab in the Incidents details dialog box. This issue has been resolved.

■ Previously, if the Lock View option on the Incident tile was enabled and the incidents were modified, the changes were reflected whenever the incidents list was refreshed. This issue has been resolved.

■ The error messages that are displayed when an invalid value is entered during Event Storage Rules creation are now descriptive and provide the essential help.

■ Previously, the exported records for some System Lookup Tables cannot be imported. This issue has been resolved.
Previously, the **Incident** tile is not displayed if the Windows Print Spool service is not running. This issue has been resolved.

- Events are now added to the same conclusion when an asset policy with multiple values is used as a tracking field in a correlation rule.

- The logic for calculating the priority of an incident in XY rule types, Symmetric Traffic rule type, and Transitive Traffic rule type is incorporated.

- If the archives are not available when you drill down a Summary Query, an appropriate error message is displayed.

- You can install Information Manager on a server having SAN attached to it. Now, you do not require to detach SAN during the installation.

## Known issues

The following are the known issues for the version 4.7.4 release of Information Manager:

- When you launch SSIM Web Start, an **Unable to launch the application** error may appear if the Java cache is not cleared or has old entries. This cache can be cleared from the Java control panel. Open Java from Control Panel. Go to **General** and click **Settings > Delete files**. Ensure that all of the options are selected and then click **OK**.

- When you launch SSIM Web Start Client, the Website certificate warning is shown twice. When this warning is displayed for the first time, check **Always trust content from this publisher**. The warning does not appear again.

- Emails that are created for a user profile from the **Notification** tab do not get deleted even after you delete the email addresses and save.

- When resource utilization is high, it may lead to issues when editing and scheduling reports. Similar issues can also occur on other areas of the Information manager console. If these issues occur, close and then re-open the Client console.

- Descriptions are not provided for some of the services that are listed in **Asset tile > Services**.

- During an Information Manager upgrade from 4.7.0 to 4.7.4, the **Onbox Agent log** file repeatedly displays error messages that show **Response code = 404**. These errors occur due to the unavailability of the url.

- After the incidents are merged the **Incident Details** pane may appear blank. Once the incidents are merged, select that merged incident to view the details on the **Incident Details** pane.
- In some cases, the SAN configuration may take an extended duration to be deleted from the Information Manager Web Configuration interface.

- When you install the Information Manager console, if the path that is provided for installation contains special characters such as /, the NSS libraries do not get initialized. In this case the server enforces FIPS communication between the server and the Information Manager console.

- In a Service Provider Manager setup, the incidents that are closed with a resolution remain listed as open incidents for some time after you refresh the screen.

- When you test a user correlation rule, the event count is not displayed correctly in the event details table.

- The / character is not permitted for a report folder name. A report folder name that is created with the / character cannot be updated.

- When you install the Information Manager client using French language, the text on the title bar gets displaced.

- When you drag and drop a query with parameters onto the dashboard, an error is displayed. Use the + (the plus symbol) to add a query with parameters to the dashboard.

- In the Information Manager console, when you select a local event archive from Events > Local Event Archives, the Help icon gets repositioned to the left side of the screen.

- When Assign to least busy user option is selected, the incidents generation rate is slightly slower than when the option is not selected. However, none of the incidents that are created when Assign to least busy user option is selected are lost. Symantec recommends you to use this option judiciously.

- Warning messages are not displayed when a lookup table that is associated with a Lookup Table Update rule is deleted. However, the corresponding warning message gets listed in the simcm.log file. The Rule gets deactivated but not reflected in the Information Manager console.

- Whenever the LDAP backup files are restored on a newly set Information Manager server, links of events associated with incidents that are generated before the LDAP restoration are broken. Symantec recommends performing the LDAP restore operation immediately after the Information Manager server is newly setup.

- If a Network File System (NFS) mounted directory is used for the LDAP and database backup through selective backup and restore, and if the NFS server is not running during the selective restore or purge of those backup files, the system may fail to respond.
If disk space is full in the /dbsesa partition, simdbmu service may stop and the user cannot log on to the Information Manager Web Configuration Interface.

When you back up a role and then assign it to a user, after restoration of that role, the role is no longer associated with that user. The same is the case with groups.

If you specify a custom path for backup file storage, then you must ensure that the db2admin user is given full permission and the sesuser is given read and execute permission.

In case the folder path where Symantec Event Agent is installed has Double Byte Character Set (DBCS), the agent does not install properly. You must ensure that the folder path has ascii characters.

When the schedule for an existing backup job is updated, a backup is triggered immediately in case the user updates the schedule with the date and time that is earlier than the current date and time.

In some cases, when a query that has the Event Date/Time parameter is run and if it contains more than 5000 events, the details of the first 5000 events are displayed. The details of the remaining events are not displayed.

The Web configuration interface does not timeout for the Event Services view and the Database Status view. This behavior occurs because the Auto Refresh functionality continuously refreshes the contents on these two pages. To ensure security for the Information Manager environment, Symantec advises you to avoid keeping the Web configuration interface in an idle and unattended condition with either of the two views open.

If you try to access a report through a URL link that is sent by email, you can access the report directly if you have already logged on to the Web configuration interface using the hostname of the Information Manager server. However if you have logged on using the IP address of the Information Manager server, then you are prompted for authentication following which the report is accessible.

Incident details from Service Provider clients using Information Manager version 4.6 MP4 cannot be opened using the custom incident filter based on hostname. The custom incident filter works correctly for the clients that are added after the setup is upgraded to 4.7.4.

If you change the date or time on the Information Manager manually or change a NTP server the self signed certificate installed on the server may become invalid, and you may not be able to logon to the console and the Web configuration interface. The Information Manager services on the server may not be able to communicate with the LDAP server.