Symantec™ Endpoint Protection Shared Insight Cache User 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 12.01.00.00

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

Symantec’s support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

**Licensing and registration**

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

www.symantec.com/business/support/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

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

Asia-Pacific and Japan  
customercare_apac@symantec.com

Europe, Middle-East, and Africa  
semea@symantec.com

North America and Latin America  
supportsolutions@symantec.com
Implementing Symantec Endpoint Protection Shared Insight Cache

This document includes the following topics:

■ About the Symantec Endpoint Protection Shared Insight Cache tool
■ How Shared Insight Cache works
■ System requirements for Shared Insight Cache
■ Installing Shared Insight Cache
■ Customizing Shared Insight Cache settings
■ Shared Insight Cache configuration file
■ Stopping and starting the Shared Insight Cache service
■ Viewing Shared Insight Cache events in the Cache Server log
■ Monitoring Shared Insight Cache performance
■ Troubleshooting issues with Shared Insight Cache
■ Uninstalling Shared Insight Cache
About the Symantec Endpoint Protection Shared Insight Cache tool

The Shared Insight Cache tool improves scan performance in virtualized environments by not scanning files that a Symantec Endpoint Protection client has determined are clean. When the client scans a file for threats and determines it is clean, the client submits information about the file to Shared Insight Cache. When any another client subsequently attempts to scan the same file, that client can query Shared Insight Cache to determine if the file is clean. If the file is clean, the client does not scan that particular file. If the file is not clean, the client scans the file for viruses and submits those results to Shared Insight Cache.

Shared Insight Cache is a Web service that runs independently of the client. However, you must configure Symantec Endpoint Protection to specify the location of Shared Insight Cache so that your clients can communicate with it. Shared Insight Cache communicates with the clients through HTTP or HTTPS. The client's HTTP connection is maintained until the scan is finished.

**Note:** Shared Insight Cache is only available for the clients that perform scheduled scans and manual scans.

For more information about how to configure Symantec Endpoint Protection Manager to communicate with Shared Insight Cache, see *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*.

See “System requirements for Shared Insight Cache” on page 9.

See “How Shared Insight Cache works” on page 8.

How Shared Insight Cache works

After the client scans a file for viruses and spyware, the client submits the scan results to Shared Insight Cache. The scan results are submitted in the form of a vote. The client submits votes for clean files only.

When Shared Insight Cache receives the vote, if the client does not have the most current virus definitions, the server ignores the vote. If newer definitions are available, the newer definitions become the latest known definitions according to Shared Insight Cache and sets the vote count to one.

When the client subsequently makes a request to Shared Insight Cache to determine if the client should scan a file, the client submits the request. Clients can submit multiple cache requests and multiple update requests in bulk. Shared Insight Cache determines if the file received greater than or equal to the vote
count threshold. If so, Shared Insight Cache returns the result of clean, which means that the client does not need to scan the file for viruses.

To keep the cache size manageable, Shared Insight Cache uses a pruning algorithm. This algorithm ensures that the cache size does not exceed the memory usage threshold. The cache pruning algorithm removes the oldest cache entries first. The oldest entries are the entries with the oldest timestamp.

**Warning:** Symantec recommends that you maintain the default prune size value in the configuration file.

See “About the Symantec Endpoint Protection Shared Insight Cache tool” on page 8.

See “Customizing Shared Insight Cache settings” on page 11.

## System requirements for Shared Insight Cache

Table 1-1 describes the system requirements that a virtual system needs to run Shared Insight Cache.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Software system requirements consist of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003/2008</td>
</tr>
<tr>
<td></td>
<td>■ .NET Framework 4</td>
</tr>
<tr>
<td>CPU size</td>
<td>Shared Insight Cache must be installed on a dedicated server or virtual machine.</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB minimum</td>
</tr>
<tr>
<td>Available disk size</td>
<td>100 MB minimum</td>
</tr>
</tbody>
</table>

See “About the Symantec Endpoint Protection Shared Insight Cache tool” on page 8.

See “Installing Shared Insight Cache” on page 9.

## Installing Shared Insight Cache

You must be a Windows administrator to install Shared Insight Cache.
Before you install Shared Insight Cache, ensure that you have met all of the system requirements.

To install Shared Insight Cache

1. On the Symantec Endpoint Protection product disc, navigate to the following folder:
   
   /Tools/SharedInsightCache/

2. Double-click on the following file to launch the installation program:
   
   msiexec /i SharedInsightCacheInstallation.msi

3. In the Shared Insight Cache Setup wizard pane, click Next.

4. Read through the Symantec Software license agreement, check I accept the terms of the License Agreement, and then click Next.

5. On the Destination Folder pane, do one of the following tasks:

   - To accept the default location for Shared Insight Cache, click Next.
   - To specify a different location for Shared Insight Cache, click Change, browse to and select the destination folder location, and click OK. Then on the Destination Folder pane, click Next.

6. On the Shared Insight Cache Settings pane, specify the following Shared Insight Cache settings:

   - Cache Usage (% of Physical Memory): Specify the maximum size of the cache. When the cache exceeds this threshold, Shared Insight Cache prunes the cache size.
   - Listening Port: The port on which the server listens.
   - Status Listening Port: The port the server uses to communicate status within the system.

7. Click Install to begin installing Shared Insight Cache.

8. Click Finish.

See “About the Symantec Endpoint Protection Shared Insight Cache tool” on page 8.
Customizing Shared Insight Cache settings

After you install Shared Insight Cache, you can customize its settings in the configuration file.

The configuration file is an XML file that follows .NET Framework application configuration standards. Shared Insight Cache does not start if there is an invalid configuration, such as invalid XML, incorrect value types, or missing required values.

Table 1-2 provides the options that you can configure and describes what each option does.

<table>
<thead>
<tr>
<th>Option</th>
<th>Type of value</th>
<th>Description</th>
<th>Restrictions and considerations</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Service Listening Port</td>
<td>Positive integer</td>
<td>Port on which the service listens</td>
<td>If the range is not between 0 - 65535, the service does not start. The service does not start if it cannot listen on the specified port.</td>
<td>9005</td>
</tr>
<tr>
<td>Status Service Listening Port</td>
<td>Positive integer</td>
<td>Port on which the service listens</td>
<td>If the range is not between 0 - 65535, the service does not start. The service does not start if it cannot listen on the specified port.</td>
<td>9006</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Percent</td>
<td>Percentage of size of the cache in megabytes (MB) before Shared Insight Cache starts pruning the cache</td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>
## Table 1-2  
**Shared Insight Cache configuration options (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Type of value</th>
<th>Description</th>
<th>Restrictions and considerations</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vote Count</td>
<td>Positive integer</td>
<td>Number of the clients that must verify that the file is clean before Shared Insight Cache uses the results</td>
<td>The value must be less than or equal to 15. If the value is greater than 15, the server uses the default value.</td>
<td>1</td>
</tr>
<tr>
<td>Log File</td>
<td>String</td>
<td>A file for the Shared Insight Cache log</td>
<td></td>
<td>&lt;installation directory&gt;/CacheServer.log</td>
</tr>
<tr>
<td>Log Level</td>
<td>Enum</td>
<td>ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF</td>
<td>A value of OFF indicates that Shared Insight Cache does not log any messages.</td>
<td>ERROR</td>
</tr>
<tr>
<td>Log Size</td>
<td>Positive integer</td>
<td>Size of the log (in bytes) until Shared Insight Cache rolls the log over</td>
<td></td>
<td>10000</td>
</tr>
<tr>
<td>Log Backups</td>
<td>Positive integer</td>
<td>Number of rolled over logs to keep before the oldest log is deleted</td>
<td>A value of 0 indicates that Shared Insight Cache retains no backups. A negative value indicates that Shared Insight Cache retains an unlimited number of backups.</td>
<td>1</td>
</tr>
<tr>
<td>Prune Size</td>
<td>Percent</td>
<td>Percentage of memory usage to remove from the cache when the cache hits the memory usage limit</td>
<td>The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value. Avoid modifying this setting.</td>
<td>10</td>
</tr>
</tbody>
</table>
To customize Shared Insight Cache settings
1. Navigate to and open the following file:
   
   Installation directory\SharedInsightCacheInstallation.exe.config
2. Make the modifications as needed.
3. Save your changes and close the file.

See “Shared Insight Cache configuration file” on page 13.
See “Installing Shared Insight Cache” on page 9.
See “About the Symantec Endpoint Protection Shared Insight Cache tool” on page 8.

Shared Insight Cache configuration file

The Shared Insight Cache configuration file is an XML file that follows the .NET application configuration standard. The installer puts the initial configuration file in the installation directory. Shared Insight Cache does not start if there is any invalid configuration including invalid XML, incorrect value types, or missing required values.

For more information about the .NET application configuration standard, go to the following URL:


The following tables describe the default configuration settings.

<table>
<thead>
<tr>
<th>Table 1-3 Service settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
</tr>
<tr>
<td>--------------</td>
</tr>
</tbody>
</table>
| Listening port | <!-- Service configuration -->  
| | </service>  
| | \<service name="CacheServer.CacheServer"  
| | behaviorConfiguration="serviceBehavior"  
| | bindingConfiguration=" serviceBinding ">  
| | <!-- address contains the ip and port -->  
| | \<endpoint address="http://localhost:9005/1"  
| | binding="webHttpBinding"  
| | contract="CacheServer.ICacheServer"  
| | behaviorConfiguration="webBehavior"/>  
| | </service>  
| | </services> |
By default the Shared Insight Cache server listens on all IP addresses. To configure the listening IP addresses for HTTP(S) services, you must use HttpCfg.exe (Windows 2003) or Netsh.exe (Windows 2008). The Shared Insight Cache server listens on the IP addresses that you specified in the IP Listen List modified by those tools.

Netsh.exe is included with Windows 2008. You can install HttpCfg.exe from the Windows 2003 installation disc. The installer is located at the following path: \\Support\Tools\Suptools.msi

For more information, go to the following URL:


<table>
<thead>
<tr>
<th>Property</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory usage</td>
<td>&lt;!-- Configure the cache itself --&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;cache.server&gt;</td>
</tr>
<tr>
<td>Vote count</td>
<td>&lt;cache.configuration vote.count=&quot;1&quot;</td>
</tr>
<tr>
<td>Prune size</td>
<td>prune.size=&quot;10&quot;</td>
</tr>
<tr>
<td></td>
<td>mem.usage=&quot;50&quot;</td>
</tr>
<tr>
<td></td>
<td>&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/cache.server&gt;</td>
</tr>
</tbody>
</table>
By default, Shared Insight cache is set up with no authentication and no SSL. It can be changed to Basic authentication with SSL, no authentication with SSL, or Basic Authentication with no SSL.
### Table 1-6 HTTP SSL and authentication settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSL</td>
<td>`&lt;webHttpBinding&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;bindingname=&quot;CacheServerBinding&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;!-- Uncomment the appropriate section to get the desired security.</td>
</tr>
<tr>
<td></td>
<td>If enabling ssl modify the uri to use https. A cert will also have to be</td>
</tr>
<tr>
<td></td>
<td>installed and registered for the ip/port.</td>
</tr>
<tr>
<td></td>
<td>--&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;!-- Basic authentication with SSL. &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;security mode=&quot;Transport&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;transport clientCredentialType=&quot;Basic&quot;/&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/security--&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;!-- No authentication with SSL. &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;security mode=&quot;Transport&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;transport clientCredentialType=&quot;None&quot;/&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/security--&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;!-- Basic authentication with no SSL. &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;security mode=&quot;TransportCredentialOnly&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;transport clientCredentialType=&quot;Basic&quot;/&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/security--&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;!-- No authentication with no SSL. DEFAULT --&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;securitymode=&quot;None&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;transportclientCredentialType=&quot;Basic&quot;/&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/security&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/binding&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/webHttpBinding&gt;</td>
</tr>
</tbody>
</table>

See “Customizing Shared Insight Cache settings” on page 11.

### Stopping and starting the Shared Insight Cache service

You may need to stop the Shared Insight Cache service temporarily to troubleshoot an issue. After you have resolved the issue, you can restart the service.

You must have Windows administrator rights to stop and start the Shared Insight Cache service.
To stop Shared Insight Cache service
◆ At the command prompt, type the following command:
    `sc stop "Shared Insight Cache"

To start Shared Insight Cache service
◆ At the command prompt, type the following command:
    `sc start "Shared Insight Cache"

To check the status of Shared Insight Cache service
◆ At the command prompt, type the following command:
    `sc query "Shared Insight Cache"

See “About the Symantec Endpoint Protection Shared Insight Cache tool” on page 8.
See “Troubleshooting issues with Shared Insight Cache” on page 20.

Viewing Shared Insight Cache events in the Cache Server log

You can view the log to see any events that Shared Insight Cache creates. Shared Insight Cache prints logs in the following format:

```
[] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message
[-]%newline
```

For example:
```
[-]
```

Modify the configuration file to specify the log severity that you want to use for Shared Insight Cache.

Table 1-7 describes the log levels that you can select.

<table>
<thead>
<tr>
<th>Log level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>OFF indicates that no incidents are logged.</td>
</tr>
<tr>
<td>Log level</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>FATAL</td>
<td>FATAL level logs the messages that require you to take action. These messages are the errors that cause Shared Insight Cache to stop. For example, a fatal message may indicate that the server IP address is not available, which means Shared Insight Cache cannot run.</td>
</tr>
<tr>
<td>ERROR</td>
<td>ERROR level logs the messages that require you to take action, but the process continues to run. They are errors in the system that cause Shared Insight Cache to fail or lose functionality. You also receive all log entries for FATAL messages. This level is the default logging level.</td>
</tr>
<tr>
<td>WARN</td>
<td>WARN level logs the messages that indicate the Shared Insight Cache behavior that may be undesirable, but do not cause it to fail. You also receive all log entries for FATAL messages and ERROR messages.</td>
</tr>
<tr>
<td>INFO</td>
<td>INFO log level messages are the messages that describe general actions or information of Shared Insight Cache. They may indicate the state of the system and help validate behavior or track down issues. However, alone they are not intended to report actionable items. For example, an information message may indicate that cache pruning is complete. The message does not detail a problem. It only logs behavior. You also receive all log entries for FATAL messages, ERROR messages, and WARN messages.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>DEBUG and ALL log level messages produce the same results. These log levels are intended for Support to troubleshoot problems with Shared Insight Cache. You also receive all log entries for all other log levels.</td>
</tr>
</tbody>
</table>

**Note:** The default setting of ERROR should be sufficient. When you increase the log, you begin to significantly increase the size of your log file. Only increase the log level when you need to troubleshoot issues with Shared Insight Cache. When you resolve the issue, return to the log level of ERROR.

### To view Shared Insight Cache events in the Cache Server log
- Go to the following directory location:

  *Installation Directory/CacheServer.log*

See “Customizing Shared Insight Cache settings” on page 11.
## Monitoring Shared Insight Cache performance

You can view statistics for Shared Insight Cache performance in the Windows performance monitor. Shared Insight Cache service must be running to view its performance.

You can view the following statistics about Shared Insight Cache's performance:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of items in the cache</td>
<td>This number represents the current number of items in the cache.</td>
</tr>
<tr>
<td>The number of items in the cache that are voted clean</td>
<td>This number represents the current number of items in the cache, which have been voted clean.</td>
</tr>
<tr>
<td>Number of cache requests</td>
<td>The number of cache requests that are made to the service. This number is only the number of valid requests that received a 200 response. This counter does not persist across restarts of the service.</td>
</tr>
<tr>
<td>Number of update requests</td>
<td>The number of update requests that are made to the service. This number is only the number of valid requests that received a 200 response. This counter does not persist across restarts of the service.</td>
</tr>
</tbody>
</table>

### To monitor Shared Insight Cache performance

1. At the command prompt, type the following command: `perfmon`

2. In the **Performance** window, right-click the graph.

3. Select **Add Counters**.

4. In the **Performance object** drop-down list, select **Shared Insight Cache**.

5. Select the counters that you want to view, and click **Add**.

6. Click **Close** to close the **Add Counters** window.

   The Shared Insight Cache counters that you selected appear in the Performance graph.

   For more information about using the Windows performance monitor, see your Windows documentation.

See “About the Symantec Endpoint Protection Shared Insight Cache tool” on page 8.
Troubleshooting issues with Shared Insight Cache

Table 1-8 provides suggestions for how to troubleshoot issues with Shared Insight Cache.

Table 1-8 Troubleshooting Shared Insight Cache

<table>
<thead>
<tr>
<th>Issue</th>
<th>Explanation/Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experiencing problems with the cache results</td>
<td>Restart the service. See “Stopping and starting the Shared Insight Cache service” on page 16.</td>
</tr>
<tr>
<td>Shared Insight Cache returns a &quot;no result&quot; response</td>
<td>Shared Insight Cache returns a no result response when it fails to successfully perform a cache lookup. If the client requests a cache lookup, a no result means that the file must be scanned for viruses. <strong>Note:</strong> Shared Insight Cache returns a success response even when it fails to successfully perform a cache update. The reason is because the client is not required to perform a different action when a failure occurs.</td>
</tr>
<tr>
<td>Suspected issues with HTTP traffic</td>
<td>View the HTTP traffic error log. The HTTP traffic errors are logged in the following location: %Windir%\System32\Logfiles\HTTPERR</td>
</tr>
</tbody>
</table>

See “Viewing Shared Insight Cache events in the Cache Server log” on page 17.
See “Monitoring Shared Insight Cache performance” on page 19.

Uninstalling Shared Insight Cache

When you no longer want to use Shared Insight Cache, you can uninstall it. Uninstalling Shared Insight Cache has the same effect as stopping the Shared Insight Cache service. If you are uncertain as to whether you want to permanently uninstall Shared Insight Cache, you can stop the Cache service instead.

When you uninstall Shared Insight Cache, ensure that you disable the Shared Insight Cache feature in Symantec Endpoint Protection. Otherwise, the Windows Event log receives notifications each time your clients cannot contact Shared Insight Cache.

You must have Windows administrator rights to uninstall Shared Insight Cache.
To uninstall Shared Insight Cache

1. In the Windows Add or Remove Programs tool, select **Shared Insight Cache**.
2. Click **Remove**.
3. Click **Yes**.

See “Stopping and starting the Shared Insight Cache service” on page 16.
Implementing Symantec Endpoint Protection Shared Insight Cache

Uninstalling Shared Insight Cache