Symantec™ Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server

Version 11.6

Symantec

Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server

Document version: 11.6a

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- 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

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:

Managed 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 is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education 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/business/services/

Select your country or language from the site index.

Contents

Chapter 1

About Integrating Microsoft ISA with Network Prevent for Web

This chapter includes the following topics:

About Network Prevent for Web integration with ISA

Microsoft Internet Security and Acceleration Server (ISA) is a security gateway product that provides both a firewall service and a Web proxy service. ISA provides no native Internet Content Adaptation Protocol (ICAP) interface, which is necessary to integrate Symantec Data Loss Prevention Network Prevent for Web with the Web proxy. However, ISA provides a Web filter architecture that enables third parties to process Web requests and responses as they are proxied.

Symantec Data Loss Prevention includes an ISA Web filter that uses ICAP to send Web requests and responses to one or more Network Prevent for Web servers for inspection. The Web filter then sends, blocks, or redacts requests and responses based on the detection result that is communicated from Network Prevent for Web.

You install and configure the Symantec Data Loss Prevention Web filter using applications that are included with Symantec Data Loss Prevention.

See "Installing and configuring the Symantec Data Loss Prevention ISA Web filter" on page 15.

Supported Network Prevent for Web functionality with ISA

The Symantec Data Loss Prevention ISA Web filter supports monitoring for the following HTTP request types:

- GET
- PUT
- POST
- GET ftp (FTP requests that are tunneled through HTTP)

The Web filter supports response monitoring for a variety of response MIME types.

See "Inspection parameters for the Symantec Data Loss Prevention Web filter" on page 30.

The Symantec Data Loss Prevention ISA Web filter does not provide monitoring for any of the following protocols:

- HTTPS
- Native FTP
- FTP PUT operations that are tunneled through HTTP

The Symantec Data Loss Prevention Web filter can send the authentication information (client credentials) of a request to Network Prevent for Web for use in logged incidents. If a user authenticates with the ISA proxy using a supported authentication mechanism, the Symantec Data Loss Prevention Web filter passes the credentials to Network Prevent for Web with the request data. If the request ultimately generates a Symantec Data Loss Prevention incident, Network Prevent for Web includes the user credential information with the logged incident data.

The Web filter can include authentication information only for the following ISA Server authentication mechanisms:

- HTTP Integrated Windows authentication
- HTTP Basic authentication
- SSL Client Certificate Authentication
- NTLM authentication

About the Symantec Data Loss Prevention Web filter

The Symantec Data Loss Prevention Web filter was developed using the Microsoft Internet Security and Acceleration Server 2004/2006 SDK. The Web filter works as an extension to the ISA Server firewall process. It registers interest in a set of notifications for performing request and/or response monitoring. The ISA firewall service calls the filter when those events occur, and it provides the associated request or response data to the filter for inspection.

The ISA Server dispatches notifications for multiple requests in parallel to all registered Web filters. However, all notifications for an individual request are processed serially. The ISA Server first passes a request notification to the highest-priority Web filter. The output of the highest-priority filter is then passed to the next-highest priority filter, and so forth, until a filter denies the requests or the final filter is executed.

The Symantec Data Loss Prevention Web filter may aggregate multiple notifications on disk to ensure that an entire request or response is delivered to Network Prevent for Web for content inspection. The Web filter holds the data and does not release it to the next filter in the chain until either:

- It receives a response from Network Prevent for Web.
- The connection to Network Prevent for Web times out. In this case, the Web filter releases the data only if the fallback action is set to **ALLOW**.
  See "Network parameters for the Symantec Data Loss Prevention Web filter" on page 27.

The ISA Server firewall process automatically loads and unloads the Symantec Data Loss Prevention Web filter at startup and shutdown.

See "Configuring the Web filter order" on page 20.

ISA requirements for Network Prevent for Web integration

The Symantec Data Loss Prevention ISA Web filter is compatible with the following ISA versions:

- Microsoft ISA Server 2004, Standard Edition or Enterprise Edition, with the latest service pack and security update
- Microsoft ISA Server 2006, Standard Edition or Enterprise Edition, with Service Pack 1 or higher and the latest security update

The Symantec Data Loss Prevention ISA Web filter also requires that you first install Microsoft .NET framework version 3.5 or higher on the ISA Server computer.

The Symantec Data Loss Prevention Web filter requires no additional system resources beyond those required by ISA itself. See the Microsoft documentation for details about ISA Server requirements.

You must configure the ISA firewall service and create access rules to permit all inbound or outbound requests and responses to pass to the Network Prevent for Web server over ICAP port 1344. Blocking or altering traffic over this port can prohibit Network Prevent for Web from inspecting data.

If you want Symantec Data Loss Prevention to record user credentials in incidents logged against ISA requests, you must configure the ISA Server with one or more compatible authentication mechanisms. See your Microsoft documentation for instructions.

See "Supported Network Prevent for Web functionality with ISA" on page 10.

Chapter 2

Installing the Symantec Data Loss Prevention Web filter

This chapter includes the following topics:

Example ISA deployment scenarios

The Symantec Data Loss Prevention Web filter can be deployed to both ISA Standard Edition and Enterprise Edition configurations. With a Standard Edition deployment, the ISA Server, Symantec Data Loss Prevention Web filter, and Symantec Data Loss Prevention Web filter configuration file all reside on the same server computer.

ISA Enterprise Edition deployments enable you to deploy logical arrays of ISA Servers to manage a different parts of your organization. For example, you may

deploy one array to manage your finance department and another array to manage your development organization.

You can deploy an ISA array to a single ISA server computer, or to multiple computers. Always install the Symantec Data Loss Prevention Web filter to each ISA Server computer in the array. You then configure the Web filter based on the number of computers in the array, and based on whether you want those computers to share the same Web filter configuration.

By default, each Symantec Data Loss Prevention Web filter installation references its own local configuration file, and therefore it maintains its own configuration. If you want multiple ISA Server computers to share the same Web filter configuration, you must configure those computers to use the same Web filter configuration file. This usually requires that you create a file share in which to store the configuration file. It also requires that you configure each remote Symantec Data Loss Prevention Web filter installation to access the file configuration file from the share.

Note: Symantec recommends that you share the configuration file from a directory of the array configuration server. You must configure the shared directory with permissions to enable each remote ISA Server computer to access the configuration file. Prepare the file share before you install the Symantec Data Loss Prevention Web filter to each ISA Server machine.

Two common ISA array configurations are as follows:

- An array resides on a single computer and shares the same Web filter configuration. The array does not share its configuration with other arrays. For this type of deployment, install the Symantec Data Loss Prevention Web filter and its configuration file to the local ISA server computer. The array accesses the local Web filter configuration file. This deployment resembles a Standard Edition deployment.
  See "Installing and configuring the Symantec Data Loss Prevention ISA Web filter" on page 15.
- An array resides on multiple ISA Server computers, but the array shares the same Web filter configuration. For this type of deployment, install the Symantec Data Loss Prevention Web filter on each ISA Server computer in the array. Then create a file share on the array configuration server to store the Symantec Data Loss Prevention Web filter configuration file for the array. Finally, configure each Web filter in the array to access the shared configuration file.
  See "Sharing a Web filter configuration file with multiple ISA Server computers" on page 37.

Installing and configuring the Symantec Data Loss Prevention ISA Web filter

Perform the following steps to install and configure the Symantec Data Loss Prevention ISA Web filter.

Table 2-1 Steps for installing the Symantec Data Loss Prevention ISA Web filter

Step	Action	Description
Step 1	Install Microsoft ISA Server.	Install a supported version of ISA. The Symantec Data Loss Prevention ISA Web filter installer requires a valid ISA Server installation to proceed. See "ISA requirements for Network Prevent for Web integration" on page 11. See your Microsoft ISA Server documentation for installation instructions.
Step 2	Install prerequisite software.	Install Microsoft .NET Framework version 3.5 or higher on the ISA Server computer. See http://www.microsoft.com/NET/ for more information. Also install the latest service pack and security update to the ISA Server computer. ISA 2006 requires Service Pack 1 or later. See http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/default.aspx for more information.
Step 3	Install and configure Network Prevent for Web.	Install and configure one or more Network Prevent for Web servers to inspect the content that will be forwarded by the Symantec Data Loss Prevention ISA Web filter, if you have not already done so. See "Example ISA deployment scenarios" on page 13.
Step 4	Configure Microsoft ISA Server.	Use the Microsoft ISA Server management utility to configure firewall policies and one or more authentication mechanisms (optional). See "About ISA Server configuration for the Symantec Data Loss Prevention Web filter" on page 16.
Step 5	Install the Symantec Data Loss Prevention ISA Web filter.	Use the Symantec Data Loss Prevention ISA Web filter installer to install the software to the ISA Server computer. For array deployments, install the Web filter on each ISA Server computer in the array. See "Installing the Web filter to ISA" on page 17.

Table 2-1 Steps for installing the Symantec Data Loss Prevention ISA Web filter *(continued)*

Step	Action	Description
Step 6	Configure the Web filter order.	The Symantec Data Loss Prevention ISA Web filter is installed as a medium-priority Web filter. If you have installed other third-party Web filters, configure the order of execution of the filters within the ISA Server. See "Configuring the Web filter order" on page 20.
Step 7	Configure the Network Prevent for Web connection and request processing.	The installer application applies a basic configuration to the Symantec Data Loss Prevention ISA Web filter. You must configure one or more Network Prevent for Web servers to use for inspection. You should also configure the exact request and response types that the Web filter forwards to Network Prevent for Web for inspection. See "Configuring Symantec Data Loss Prevention Web filter connections and inspection behavior" on page 21.

About ISA Server configuration for the Symantec Data Loss Prevention Web filter

The ISA Server firewall limits the requests and responses that are subsequently processed by the ISA Server Web proxy service. You can limit network traffic by protocol and by user permissions. Traffic that is permitted through the firewall is then passed to the ISA Server Web proxy, and can be subsequently processed the Symantec Data Loss Prevention Web filter.

Configure the ISA firewall service as necessary for our deployment.

Note: You can configure firewall policies before or after installing the Symantec Data Loss Prevention ISA Web filter. As a best practice, ISA Server should send only authorized network traffic to Network Prevent for Web for inspection. The firewall service provides the first and most efficient way to limit the network traffic that is sent to Network Prevent for Web.

If you want to record user client credentials in Symantec Data Loss Prevention incidents, also configure a compatible ISA Server authentication mechanism. If a user authenticates with the ISA proxy using a supported authentication mechanism, the Symantec Data Loss Prevention Web filter passes the credentials to Network Prevent for Web along with the request data. If the request ultimately generates a Symantec Data Loss Prevention incident, Network Prevent for Web includes the user credential information with the logged incident data.

See "Supported Network Prevent for Web functionality with ISA" on page 10.

See your Microsoft ISA Server documentation for information about configuring firewall rules, disabling Web caching, and configuring an authentication mechanism.

Installing the Web filter to ISA

Follow these steps to install the Symantec Data Loss Prevention ISA Web filter to an ISA server.

To install the Symantec Data Loss Prevention ISA Web filter

1. Copy the installer application, `symc_isa_plugin.msi`, to the ISA Server computer machine on which you want to install the Web filter. This file is located in the *`DLPDownloadHome`*`\Symantec_DLP_11_Win\New Installs\ISA` or *`DLPDownloadHome`*`/Symantec_DLP_11_Lin/New Installs/ISA` directory, where *`DLPDownloadHome`* is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.

   You must execute the Web filter installer directly on the ISA Server computer.
2. Double-click the `symc_isa_plugin.msi` file to begin the installation process. The installer loads and displays a welcome screen.
3. Click **Next** to display the **End-User License Agreement** screen.
4. Accept the license agreement and click **Next** to display the **Web Filter Monitoring Options** screen.
5. Select a monitoring option for the initial Web filter configuration, then click **Next**.

Monitoring option	Description
Request Monitoring	The Web filter sends Web requests to Network Prevent for Web for inspection. This installer option configures the filter to inspect only PUT and POST operations. See "Inspection parameters for the Symantec Data Loss Prevention Web filter" on page 30. **Note:** Do not inspect GET requests unless absolutely required. Enabling GET request inspection causes nearly all HTTP traffic to flow through the filter to Network Prevent for Web. This may delay request processing on the ISA Server, and sensitive data is rarely lost in GET requests.

Monitoring option	Description
Response Monitoring	The Web filter sends Web responses to Network Prevent for Web for inspection. This installer option configures response monitoring only for the following MIME types: ■ application/msword ■ application/octet-stream ■ application/pdf ■ application/postscript ■ application/vnd.ms-excel ■ application/vnd.ms-powerpoint ■ application/vnd.ms-project ■ application/vnd.ms-works ■ text/html ■ text/plain ■ text/richtext ■ text/scriptlet ■ text/tab-separated-values ■ text/webviewhtml ■ text/x-component ■ text/x-setext ■ text/v-card ■ text/xml To inspect the content of other response MIME types, use the Web filter configuration utility after installation. **Note:** Use discretion when selecting additional MIME types, as this can place increased loads on the Web filter and Network Prevent for Web and may delay processing of responses on the ISA Server. See "Inspection parameters for the Symantec Data Loss Prevention Web filter" on page 30.
Both	The Web filter sends both requests and responses to Network Prevent for Web as described above. **Note:** Do not select this option unless both request and response monitoring are required. Monitoring both requests and responses can place increased loads on the Web filter and on Network Prevent for Web, which can slow the processing of requests and responses on the ISA Server.

Monitoring option	Description
None	The Web filter sends no requests or responses to Network Prevent for Web for inspection. If you choose this option, you must use the Web filter configuration utility to select monitoring options after installation. See "Inspection parameters for the Symantec Data Loss Prevention Web filter" on page 30.

The installer displays the **ISA Config Server location** screen.

6 Select one of the following options based on the ISA Server edition you use, then click **Next**:

Option	Description
ISA config server is installed locally on this machine	Select this option in either of the following cases: ■ You are installing on a Standard Edition ISA Server computer. ■ You are installing on an Enterprise Edition ISA Server computer and the ISA configuration server is located on the same computer.
ISA config server is installed on a remote machine	Select this option if you are installing on an Enterprise Edition ISA Server computer that uses a remote ISA configuration server. The installer prompts you to enter the address of the ISA configuration server computer. Note that you must install the Web filter on the ISA Server computer and not on the remote ISA configuration server computer.

Note: If you install using the wrong option, you must uninstall and then reinstall the Symantec Data Loss Prevention ISA Web filter to correct the problem.

7 If you are installing to a local ISA configuration server, skip this step.

On the **User Information** screen, enter the DNS name or IP address of the remote ISA configuration server computer, then click **Next**.

8 After the installer indicates that it is ready to install the Web filter plug-in, click **Install**.

9 After the installer completes the installation, click **Finish** to exit the installer.

Configuring the Web filter order

The Symantec Data Loss Prevention Web filter operates at a medium priority, which is the Microsoft recommendation for all third-party Web filters. This ensures that the filter receives content that has already been decompressed by the ISA Server decompression filter (which is necessary for content inspection). Your ISA Server deployment may contain multiple medium-priority Web filters. In this case, you must choose which third-party filters are executed before others.

Always deploy the Symantec Data Loss Prevention Web filter after any Web filters that perform URL filtering or authorization. This ensures that you inspect content with Network Prevent for Web only if the request is fully authorized by other filters. For example, if you deploy Symantec Web Security for Microsoft Internet Security and Acceleration (ISA) Server 2004, place that Web filter before the Symantec Data Loss Prevention Web filter in the list of medium-priority filters. This ensures that you do not perform DLP inspection on content that may ultimately be blocked by URL filtering policies.

Follow these steps to change the order of execution for the Symantec Data Loss Prevention Web filter:

To change the order of execution for the Web filter

1. Log on to the **ISA Server Management** console for the ISA Server deployment you want to configure.
2. Select the ***server_name*** **> Configuration > Add-ins** node in the left pane, where ***server_name*** is the name of your ISA configuration server.
3. Select the **Web Filters** tab in the right pane.
4. Click the **SYMC ISA Web Filter for DLP** in the list of installed Web filters.
5. Use the up and down arrows to change the order of the **SYMC ISA Web Filter for DLP** in relation to other medium-priority Web filters. For example, ensure that the Symantec Data Loss Prevention Web filter executes after URL filters or authentication filters, such as Symantec Web Security for Microsoft Internet Security and Acceleration.

   Note: You can only re-order the Symantec Data Loss Prevention Web filter in relation to other medium-priority filters.

6. Click **Apply** to apply your changes.
7. Click **OK** to acknowledge the change.
8. Select **File > Exit** to exit the management console.

Configuring Symantec Data Loss Prevention Web filter connections and inspection behavior

After installation, you must configure Symantec Data Loss Prevention Web filter with one or more Network Prevent for Web servers for content inspection. You may also choose to perform the following configuration tasks:

- Modify the default request and response types that are sent to Network Prevent for Web for inspection. (Default values are chosen based on your selection during the installation process.)
- Set the default action that the Web filter performs when it cannot connect to Network Prevent for Web for inspection. By default, the Web Filter allows all requests and responses to proceed if it cannot reach a Network Prevent for Web server.

The following procedure describes how to perform these post-installation configuration tasks.

Note: The **Symantec ISA Web Filter Plugin Configuration** utility also enables you to configure features such as network connection parameters and logging capabilities. The default values for these configuration parameters are usually sufficient for all installations.

See "Symantec Data Loss Prevention Web filter configuration parameters" on page 25.

To configure the Symantec Data Loss Prevention Web filter after installation

1. Log in to the configuration server for your Microsoft ISA Server installation.
2. Select **Start > Run** and enter the path to the Web filter configuration utility: `C:\Program Files\Microsoft ISA Server\symc_isa_plugin_gui.exe`.
3. Select the **Prevent** tab.
4. Double-click the first empty box under the **Web Prevent** column, and type the DNS name or IP address and port number of a Network Prevent for Web to which the Web filter forwards requests or responses for inspection. Separate the address and port number with a colon. For example, enter `webprevent.mycompany.com:1344`.

5 Repeat the previous step if you use multiple Network Prevent for Web servers. The Web filter automatically load balances between configured Network Prevent for Web servers by forwarding each request to the server that has the least load.

The filter calculates the load by first polling configured Network Prevent for Web servers to determine each the ICAP connection limit of each server (if the filter is not configured to override the limit). The filter then computes the current capacity of each server based on the number of outstanding requests and the advertised capacity of the server. It orders the servers by current capacity, and chooses servers in ascending order until it establishes a connection.

Note: The **Connection Override** is used to reduce the maximum number of ICAP connections to a Network Prevent for Web server in deployments where multiple Web filters send requests to the same Network Prevent for Web server.

See "Network Prevent for Web connection parameters for the Symantec Data Loss Prevention Web filter" on page 33.

---

6 Select the **Inspection** tab. The configuration utility displays the available request types and response MIME types that the Web filter can send to Network Prevent for Web for inspection.

7 Select or unselect request types and response MIME types as necessary for your deployment.

8 Select the **Network** tab to display network connection properties and the default Web filter action.

9 In the **Fallback Action** menu, select the action that the Web filter performs when it cannot connect to a Network Prevent for Web server for inspection:

ALLOW	The Web filter allows the request or response to pass without Symantec Data Loss Prevention inspection. All aggregated notifications are passed to the next ISA Web filter for processing.
BLOCK	The Web filter blocks the request or response and lower priority filters do not see the request or response.

10 Click **OK** to apply your changes and exit the configuration utility. Your changes take effect immediately, and you do not need to restart the firewall service.

See "Symantec Data Loss Prevention Web filter configuration parameters" on page 25.

Uninstalling the Symantec Data Loss Prevention Web filter

Follow these steps to uninstall the Symantec Data Loss Prevention Web filter from an ISA Server computer.

Note: If you use a non-default location to share the Web filter configuration file, the uninstallation process does not remove that file. You must manually remove any non-default configuration file.

Note: When you uninstall the Symantec Data Loss Prevention Web filter for ISA, the uninstall process restarts the ISA firewall service. This restart is required because the Web filter DLL cannot be removed until the firewall service relinquishes control of the DLL. Because uninstalling the Web filter is disruptive to the ISA firewall service, schedule the uninstall procedure during off-peak hours or during a previously scheduled maintenance period.

To uninstall the Web filter from an ISA Server computer

1. Log on to an ISA Server computer where you have installed the Symantec Data Loss Prevention Web filter.
2. Select **Start > Control Panel > Add or Remove Programs**.
3. Select the Symantec ISA Web Filter Plugin entry from the list of installed programs.
4. Click **Remove**.
5. Click **Yes** to verify that you want to remove the software.

   The application uninstalls the Symantec Data Loss Prevention Web filter software.

Chapter 3

Configuring the Symantec Data Loss Prevention Web filter

This chapter includes the following topics:

Symantec Data Loss Prevention Web filter configuration parameters

The Symantec Data Loss Prevention Web filter stores all of its configuration information in a dedicated file, `isa_plugin.conf`. The configuration file resides in the ISA configuration server installation directory, `C:\Program Files\Microsoft ISA Server` where *C* is the drive letter of the installation. Always use the **Symantec ISA Web Filter Plugin Configuration** utility, located at `C:\Program Files\Microsoft ISA Server\symc_isa_plugin_gui.exe`, to change the Web filter configuration. The Web filter automatically applies any

changes you make using the configuration utility when you click **Apply** or **OK**. You do not need to restart the firewall service for the changes to take effect.

The configuration utility is divided into several tabs, each of which enables you to configure different aspects of the Web filter's behavior.

Table 3-1 Web filter configuration utility tabs

Web filter configuration tab	Description	Additional information
Network	Configures the network connection between the Web filter and Network Prevent for Web servers. Also configures the default action that the Web filter performs when it cannot connect to Network Prevent for Web.	See "Network parameters for the Symantec Data Loss Prevention Web filter" on page 27.
Logging	Configures the location and contents of Web filter log files.	See "Logging parameters for the Symantec Data Loss Prevention Web filter" on page 29.
Inspection	Defines the request types and response MIME types that the Web filter sends to Network Prevent for Web for inspection.	See "Inspection parameters for the Symantec Data Loss Prevention Web filter" on page 30.
Buffer	Configures the buffering parameters that are used to stream data between ISA and Network Prevent for Web. **Note:** Use the default values for these configuration parameters unless a Symantec support representative instructs you to change them.	See "ISA Server buffer parameters for the Symantec Data Loss Prevention Web filter" on page 32.

Table 3-1 Web filter configuration utility tabs *(continued)*

Web filter configuration tab	Description	Additional information
Prevent	Defines the connection properties for one or more Network Prevent for Web servers. The Web filter automatically load balances between multiple configured Network Prevent for Web servers.	See "Network Prevent for Web connection parameters for the Symantec Data Loss Prevention Web filter" on page 33.

Network parameters for the Symantec Data Loss Prevention Web filter

Use the **Network** tab of the Symantec Data Loss Prevention Web filter configuration utility to configure properties of the network connection between the Web filter and Network Prevent for Web servers. You can also use this tab to set the default action that the Web filter performs when it cannot connect to Network Prevent for Web.

Table 3-2 Network configuration parameters

Parameter name	Default value	Description
Connection Timeout	60 seconds	The maximum amount of time that the Web filter waits to establish a TCP connection to a Network Prevent for Web server. If no response is received after the timeout value, the filter considers the connection attempt as failed and takes the **Failback Action** described below.
Hold Timeout	5 seconds	The maximum amount of the time that the Web filter waits before it re-attempting a TCP connection to Network Prevent for Web, either because of a TCP connection timeout or because of the server's ICAP connection limit. The filter holds pending requests and responses during this time.

Table 3-2 Network configuration parameters *(continued)*

Parameter name	Default value	Description
Read/Write Timeout	60 seconds	The maximum amount of time that the Web filter waits for a response when it sends or receives data from Network Prevent for Web. For example, if the filter successfully sends a request to Network Prevent for Web for inspection, it by default waits a maximum of 60 seconds for Network Prevent for Web to respond with the inspection result. If no response is received in this amount of time, the filter returns an error, which effectively blocks other filters from seeing the data. If this occurs, the end user would need to retry their request.
Fallback Action	ALLOW	Defines the action that the Web filter performs when it cannot connect to a Network Prevent for Web server for inspection, or if the Network Prevent for Web server does not respond within the **Hold Timeout** duration: ■ **ALLOW** allows the request or response to pass without Symantec Data Loss Prevention inspection. All aggregated data is passed to the next ISA Web filter for processing. ■ **BLOCK** blocks the request or response.
Connection Retries	1	The number of times the Web filter tries to reconnect to a Network Prevent for Web server if the TCP connection fails or if the detection server ICAP connection limit was reached.
TCP Send Buffer Size	65535 bytes	The size of the TCP send buffer that the Web filter uses to communicate with Network Prevent for Web servers. If the value you specify causes a failure, the Web filter uses the value of 8 KB instead of the configured value.

Table 3-2 Network configuration parameters *(continued)*

Parameter name	Default value	Description
TCP Receive Buffer Size	65535 bytes	The size of the TCP receive buffer that the Web filter uses to communicate with Network Prevent for Web servers. If the value you specify causes a failure, the Web filter uses the value of 8 KB instead of the configured value.

Logging parameters for the Symantec Data Loss Prevention Web filter

Use the **Logging** tab of the Symantec Data Loss Prevention Web filter configuration utility to configure the location, number, and contents of Web filter log files.

Table 3-3 Logging configuration parameters

Parameter name	Default value	Description
Log Directory	*C*:\Program Files\Microsoft ISA Server\symc_isa_plugin_logs	Specifies the directory location in which to store Web filter log files.
Log File Name	symc_isa_plugin.log	Specifies the name format for Web filter log files. For multiple log files, the Web filter appends a number to the end of the log file name you specify. For example: `symc_isa_plugin.log.1`, `symc_isa_plugin.log.2`, and so forth.
Log File Size	104857600 bytes	The maximum size of a single log file. After this size is reached, the Web filter begins writing to another log file, up to the maximum number of configured log files.
Maximum Number Of Log Files	10	The maximum number of Web filter log files to create. After the maximum number of files is reached, the Web filter overwrites log files beginning with the earliest file number.

Table 3-3 Logging configuration parameters *(continued)*

Parameter name	Default value	Description
Logging Level	FINE	The level of detail to include in Web filter log files. The available options are: ■ FINE ■ FINER ■ FINEST

Inspection parameters for the Symantec Data Loss Prevention Web filter

Use the **Inspection** tab of the Symantec Data Loss Prevention Web filter configuration utility to select the request types and response MIME types that the Web filter sends to Network Prevent for Web for inspection. If a type is not selected on this page, the Web filter simply passes the data associated with the ISA Server notification to the next Web filter for processing (without aggregating the data). Notifications that contain requests or responses of selected types are aggregated on disk to ensure that the entire request or response is passed to Network Prevent for Web for inspection.

Note: Do not perform both request and response monitoring unless absolutely required. Monitoring both requests and responses can place increased loads on the Web filter and on Network Prevent for Web, which can slow the processing of requests and responses on the ISA Server.

See "ISA Server buffer parameters for the Symantec Data Loss Prevention Web filter" on page 32.

Table 3-4 Inspection configuration parameters

Parameter name	Default values	Description
Request Types	The following default request types are selected if you select **Request Monitoring** or **Both** during the Symantec Data Loss Prevention Web filter installation: ■ PUT ■ POST	Specifies whether the Web filter should forward GET, PUT, POST, or GET ftp requests. Because GET requests can generate large volumes of network traffic, by default the Web filter does not send GET requests for inspection. If you choose to inspect GET requests, see the *Symantec Data Loss Prevention Administration Guide* for guidelines on enabling GET processing. See ISA Server buffer parameters for the Symantec Data Loss Prevention Web filter on page ?.

Table 3-4 Inspection configuration parameters *(continued)*

Parameter name	Default values	Description
Response MIME Types	The following default MIME types are selected if you select **Response Monitoring** or **Both** during the Symantec Data Loss Prevention Web filter installation: ■ application/msword ■ application/octet-stream ■ application/pdf ■ application/postscript ■ application/vnd.ms-excel ■ application/vnd.ms-powerpoint ■ application/vnd.ms-project ■ application/vnd.ms-works ■ text/html ■ text/plain ■ text/richtext ■ text/scriptlet ■ text/tab-separated-values ■ text/webviewhtml ■ text/x-component ■ text/x-setext ■ text/v-card ■ text/xml	Specifies which MIME types the web filter forwards to Network Prevent for Web for inspection. **Note:** Use discretion when selecting MIME types. Each additional MIME type places increased loads on the Web filter and Network Prevent for Web. This may delay processing of responses on the ISA Server.

ISA Server buffer parameters for the Symantec Data Loss Prevention Web filter

Use the **Buffer** tab of the Symantec Data Loss Prevention Web filter configuration utility to control details of the interface between the ISA Server and the Symantec Data Loss Prevention Web filter.

The Symantec Data Loss Prevention Web filter may aggregate multiple ISA Server notifications on disk to ensure that an entire request is delivered to Network Prevent for Web for content inspection. The Web filter aggregates all notification data until it receives an end of request or end of response notification from ISA. Filters that are lower in priority do not receive notifications until the complete request has been submitted to and approved by Network Prevent for Web.

Table 3-5 Buffer configuration parameters

Parameter name	Default value	Description
Stream Buffer Size	10485760 bytes	Defines the maximum amount of data that the Web filter writes back to ISA at one time, after Network Prevent for Web has approved a request or response. This parameter affects the way in which the next Web filter receives the data for processing. Consider an example where the Web filter aggregates a 10 megabyte request and sends it to Network Prevent for Web for inspection, and the detection server approves the request. With the default value of **Stream Buffer Size**, the Web filter sends the approved request data to the next Web filter in 10 MB chunks.
ISA Retry Count	0	Specifies the number of times the Web filter will try to push approved request data to ISA if a failure occurs.

Network Prevent for Web connection parameters for the Symantec Data Loss Prevention Web filter

Use the **Prevent** tab of the Symantec Data Loss Prevention Web filters configuration utility to define the connection properties for one or more Network Prevent for Web servers. The Web filter automatically load balances between multiple configured Network Prevent for Web servers.

Table 3-6 Prevent configuration parameters

Parameter name	Default value	Description
Web Prevent	n/a	Specifies the IP address or DNS name and port number of a Network Prevent for Web server to monitor requests and responses. For example: webprevent.mycompany.com:1344. If you define multiple Network Prevent for Web servers, the Web filter automatically load balances to all servers by forwarding new requests and responses to the server with the least current load. **Note:** Other Web filters or Web proxies that access the Network Prevent for Web server may generate additional load that is not considered in the load-balancing algorithm.

Table 3-6 Prevent configuration parameters *(continued)*

Parameter name	Default value	Description
Connection Override	0	The **Connection Override** parameter enables you to reduce the ICAP connection limit for a configured Network Prevent for Web server. Reducing the connection limit may be required if multiple ICAP clients (such as multiple Web filters or Web proxies) use the same Network Prevent for Web server for inspection. If you specify a non-zero value, the Web filter uses that value as the ICAP connection limit, rather than the connection limit that is advertised by the Network Prevent for Web server. If you specify zero (the default value), the Web filter uses the connection limit advertised by the server. (The filter obtains the connection limit once in every interval defined by the **Health Check Timeout** parameter, described below.) By default a single Network Prevent for Web server supports a maximum of 25 simultaneous ICAP connections. However, each ICAP client to the server may create multiple ICAP connections to the server, up to the advertised limit. If you integrate multiple Symantec Data Loss Prevention Web filters or proxies with the same Network Prevent for Web server, each ICAP client receives the same advertised connection limit. Such a configuration can quickly overload the Network Prevent for Web server unless you reduce the advertised connection limit or use the **Connection Override** parameter. The **Connection Override** parameter enables you to configure each Web filter independently of others. For example, you can configure those Web filters that process the most traffic to consume additional ICAP connections. Web filters that process very little traffic can be configured to use fewer connections. This configuration balances the resources that are required to maintain ICAP connections on the Network Prevent for Web server. **Note:** You can optionally change the connection limit that the Network Prevent for Web server advertises. However, you must restart the Network Prevent for Web server for the change to take effect. See the Enforce Server administration console online Help for more information.
Health Check Timeout	30 seconds	Configures the frequency with which the Symantec Data Loss Prevention Web filter polls each Network Prevent for Web server for ICAP connection properties, such as the ICAP connection limit.

Appendix A

Configuring the Web filter for ISA arrays

This appendix includes the following topics:

Sharing a Web filter configuration file with multiple ISA Server computers

This release of the ISA Web filter installer does not prompt you for a location to store the configuration file. Instead, each Web filter installation uses a dedicated configuration file that is stored in a default location on the local ISA Server computer.

Multiple ISA Server computers in an array, or multiple ISA arrays, may share a common configuration. If you want to share the Symantec Data Loss Prevention Web filter configuration with multiple ISA Server computers or multiple arrays, each Web filter installation should reference the same Web filter configuration file. This practice helps you to maintain a single Web filter configuration without having to configure each Web filter independently. As you make changes to the Web filter configuration from any computer, the changes are automatically propagated to each Web filter installation that references the file share.

Symantec recommends that you create a directory on an array configuration server to hold the shared configuration file. Then share the configuration file location to all other ISA servers computers that require the same configuration.

Perform the following steps to prepare a file share and configure the Web filter to use a non-default configuration file.

Note: As an alternative, you can configure each Web filter installation independently, or manually copy a master configuration file to the default configuration file location on each local ISA Server computer. This practice may be acceptable if you have only a few ISA Server computers that share the same configuration.

Step	Action	Description
Step 1	Prepare the shared configuration file.	Install and configure the Symantec Data Loss Prevention Web filter on a single ISA server computer. Configure the filter using the options that you want to share with other ISA Server computers in the array, or with other arrays. You will use this server's configuration file as the master configuration file and copy it to the file share you prepare in Step 2. See "Installing and configuring the Symantec Data Loss Prevention ISA Web filter" on page 15.
Step 2	Prepare the share directory.	Create a shared directory on the ISA configuration server to hold the Web filter configuration file. Configure the security settings of the share so that remote ISA server computers can access it. See "Preparing a shared directory for remote ISA Server computers" on page 39.
Step 3	Install and configure Symantec Data Loss Prevention Web filters to access the shared configuration file.	Install the Symantec Data Loss Prevention Web filter on other, remote ISA server computers. To configure these Web filter installations to use the shared configuration file, use the `regedit` utility to set the configuration file location. See "Configuring a Symantec Data Loss Prevention Web filter installation to use a non-default configuration file" on page 40.

Preparing a shared directory for remote ISA Server computers

Follow these steps to create a shared directory in which to store the master Web filter configuration file.

To prepare a shared directory for the master Web filter configuration file

1. Log into the ISA configuration server for the array that will store the Web filter configuration file.
2. Create the share directory in which you will store the configuration file. For example:

   ```
   mkdir c:\share_isa
   ```

3. Using Windows Explorer, right-click the new directory and select **Properties**.
4. Click the **Security** tab.
5. Click **Advanced**.
6. Deselect the option: **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.**
7. When the **Security** dialog box appears, click **Copy**.
8. Click **OK** to apply your changes and dismiss the **Advanced Security Settings** dialog box.
9. Click **Add** to open the **Select Users or Groups** dialog box.
10. Click **Object Types** and ensure that the **Computers** option is selected. Click OK to dismiss the **Object Types** dialog box.
11. In the **Enter the object names to select** field, specify the ISA Server computers that need to access the file share (for example ***Domain\IAS_Computer1***, ***Domain\IAS_Computer2*** and so forth). You must provide authenticated access and read privileges for each remote ISA server computer that will access the share. Use the **Check Names** option to verify your entries.
12. Click **OK** to apply your changes.
13. Select a computer name that you added in Step 11.
14. In the **Permissions for *computer_name*** section, select the **Allow** checkbox for the **Read** permission. If you want to allow modification of the configuration file from this computer, also allow the **Write** permission.
15. Click **Apply**.

16 Repeat Steps 13 - 15 for each ISA Server computer that must access the share.

17 Click the **Sharing** tab.

18 Click select the **Share this folder** option.

19 Click **Permissions**.

20 Click **Add** to open the **Select Users, Computers, or Groups** dialog box.

21 Type **Authenticated Users** in the **Enter the object names to select** field, and click **Check Names**.

22 Click **OK**.

23 In the **Permissions for share_isa** dialog box, select the **Authenticated Users** entry.

24 Select the **Allow** checkbox for the **Full Control** permission.

25 Select the **Everyone** group, and click **Remove**.

26 Click **OK** to dismiss the permissions dialog.

27 Click **OK** to dismiss the share properties dialog.

28 Install the Symantec Data Loss Prevention Web filter on at least one ISA server in the array. Configure that filter as necessary for the array as a whole.

29 Copy the master Web filter configuration file to the shared directory. For example:

```
copy c:\Program Files\Microsoft ISA Server\isa_plugin.conf \\config_server\share_isa
```

Configuring a Symantec Data Loss Prevention Web filter installation to use a non-default configuration file

By default, a Symantec Data Loss Prevention Web filter looks for its configuration file in the `c:\Program Files\Microsoft ISA Server` directory. Follow these instructions to configure the Web filter to use the master configuration file on the file share you prepared.

To configure the Web filter to use a non-default configuration file

1 Log on to an ISA Server computer where you have installed the Symantec Data Loss Prevention Web filter.

2 Select **Start > Run** and enter `regedit`.

3 In the left pane, select **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\symc isa plugin**.

4 In the right pane, double-click **config file path** to open the **Edit String** dialog for this key.

5 Change the **Value data** field to:

`\\configuration_server\directory_name`

Replace *configuration_server* with the name of the ISA configuration server (for example, `\\config_server\share_isa`). Replace *directory_name* with the name of the folder that contains the master Symantec Data Loss Prevention Web filter configuration file (`isa_plugin.conf`).

6 Click **OK** to accept the change.

7 Select **File > Exit** to exit the registry editor.

8 You must restart the ISA firewall process to use the new Web filter configuration file path. Select **Start > Run** and enter `services.msc`.

9 Select **Microsoft Firewall** from the list of services.

10 Click **Restart** to restart the firewall and use the shared Web filter configuration file.

11 Select **File > Exit** to exit the Services utility.

Index

R

S

T

V

W