Administrator Help

Websense Email Security

v7.2

Published September 9, 2009
Printed in the United States of America and Ireland.

RSA MD5 by RSA Data Security (Open Source)

The Apache Software License, Version 1.1

The Apache Software License, Version 2.0

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

OpenSSL

This product includes software developed by the OpenSSL project. Use of the OpenSSL is governed by the OpenSSL license:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SSLeay

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. That is, this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

OddButton

Copyright © 2001-2002 Paolo Messina and Jerzy Kaczorowski

The contents of this file are subject to the Artistic License (the "License"). You may not use this file except in compliance with the License. You may obtain a copy of the License at:

http://www.opensource.org/licenses/artistic-license.html

THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT

LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

You can download a copy of the unmodified code from

http://www.codeproject.com/buttonctrl/oddbutton.asp

ICU License - ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Contents

1 Introduction

About Websense Email Security

Websense Email Security is an on-site, server-based application that provides connection management and content filtering for inbound and outbound email. The solution easily and flexibly allows you to implement an Acceptable Use Policy (AUP) for email by:

1. Scanning the content, sender, destination, attachments and size of all email to and from the Internet.
2. Applying rules that you have established to support your AUP.

Websense Email Security is comprised of the following core components:

- **Dashboard** – The Dashboard provides a real-time picture of Websense Email Security system status, including active components, connection status, filtering activity, and alert conditions.
- **Monitor** – The Monitor shows the progress of email through Websense Email Security in real-time. It indicates server status and the number of messages in each queue. It also provides access to other component user interfaces.
- **Rules Administrator** – The Rules Administrator is used to set up the rules that meet the needs of your AUP. Configuring rules requires careful planning initially, but is then easy to set up and apply.

  If an email triggers a rule, Websense Email Security uses the actions specified in the rule to delay, discard, or isolate the email. Delayed or isolated messages are placed in dedicated queue folders. If an email does not trigger a rule, it is placed in a folder for delivery to its destination.
- **Message Administrator** – The Message Administrator is used to review, manage and analyze email that has been placed in queue folders, and view logs of Websense Email Security activity.

Websense Email Security includes additional components that enhance the capabilities of the Websense Email Security core components. For more information, see *Additional components*, page 24.

Report Central

Report Central is used to create Websense Email Security activity reports. See the *Report Central Administrator's Guide* for details.

Personal Email Manager

Personal Email Manager monitors queues that you specify and sends end-users periodic notification email listing their blocked messages. It also allows users to manage their blocked email. See the *Personal Email Manager Administrator's Guide* for details.

Subscription key

To use Websense Email Security past the 30-day evaluation period, you must purchase a subscription. To purchase a subscription, contact your Websense Email Security Reseller or your Websense Sales Representative. For contact information, go to: http://www.websense.com/global/en/AboutWebsense/ContactUs/

When you purchase a subscription you will receive a *subscription key.* Keep a record of your key in a place where it is easy to retrieve. You will need it when installing the software and when contacting Websense Technical Support. If the software is already installed, open the Monitor to enter your key or view the status and expiration date of the key. On the Monitor menu bar select **About > Websense Email Monitor**. To enter your key, click **Subscribe**. The **Subscribe** feature is not available from a remote client.

Your subscription key enables email filtering and several ThreatSeeker technologies, including:

- Anti-Spam Agent
- Virtual Learning Agent
- Anti-Virus Malware Scanning
- Internet Threat Database

Optionally, you can extend your subscription to include:

- Anti-Virus Agent
- Virtual Image Agent (VIA)

Anti-Virus Agent uses a McAfee scanning engine to protect your organization from email-borne viruses. It works together with the Websense Anti-Virus Malware Scanning component to provide maximum email security from viruses.

Virtual Image Agent is an image-recognition tool that isolates email that contains explicit adult images, helping to reduce potential legal liabilities.

All of your subscribed services are encoded in a single subscription key.

Online Help

Select the **Help** option within the program to display detailed information about the product.

Important

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

Related topics

- *Finding a Help topic*, page 17
- *Bookmarking a topic*, page 17
- *Copying a Help topic*, page 18
- *Printing a Help topic*, page 18
- *Opening the Help PDF file*, page 18

Finding a Help topic

In the Help viewer, select one of the tabs:

- **Contents**

  Double-clicking a book icon expands that book.

  Click a table of contents entry to display the corresponding topic.

- **Index**

  Select a letter and scroll through the list. Topics may be indexed with more than one entry.

  Double-click an entry to display the corresponding topic.

- **Search**

  Enter a word or phrase and click **Go**.

  Click an entry of the results list to display the corresponding topic.

Bookmarking a topic

You can create a list of Help topics by bookmarking them:

1. Use the **Contents**, **Index**, or **Search** tab to locate and display the topic you want to bookmark.
2. Click the **Favorites** tab and click **Add**.

Copying a Help topic

You can copy a Help topic and paste it into another file, for example, a Word document:

1. In the topic pane of the browser, right-click and click **Select All** on the shortcut menu.
2. Still inside the topic pane, right-click again and click **Copy**.
3. The topic is copied to the Clipboard.
4. Open the document and use the Paste function to include the copied text. Some applications provide a Paste Special function in which you can select the type of text to insert (HTML, RTF, plain text, etc.).

Printing a Help topic

To print a Help topic:

1. Use the **Contents**, **Index,** or **Search** tab to locate and display the topic you want to print.
2. Click the Print icon on the right side of Help toolbar.
3. The **Print** dialog box displays.
4. Click **Print**.

Alternatively, open the PDF version of the Administrator's Guide, navigate to the topic you want to print and select **File > Print**. Specify the page or pages to print.

Opening the Help PDF file

To open the Help PDF file, click the Adobe Acrobat PDF icon at the top of the topic in the upper right corner. The PDF contains all of the Help topics in the online system as well as some additional information.

Technical Support

Technical information about Websense products is available 24 hours a day at:

www.websense.com/support/

- latest release information
- searchable Websense Knowledge Base
- show-me tutorials

- product documents
- tips
- answers to frequently asked questions
- in-depth technical papers

For additional questions, click the Contact Support tab at the top of the page and fill out the online support form.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

Location	Contact information
North America	+1 858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1 858-458-2940

For telephone requests, please have ready:

- Websense subscription key
- Access to Websense Email Security and its components
- Familiarity with your network's architecture, or access to a specialist
- Specifications of machines running Websense Email Security and its components

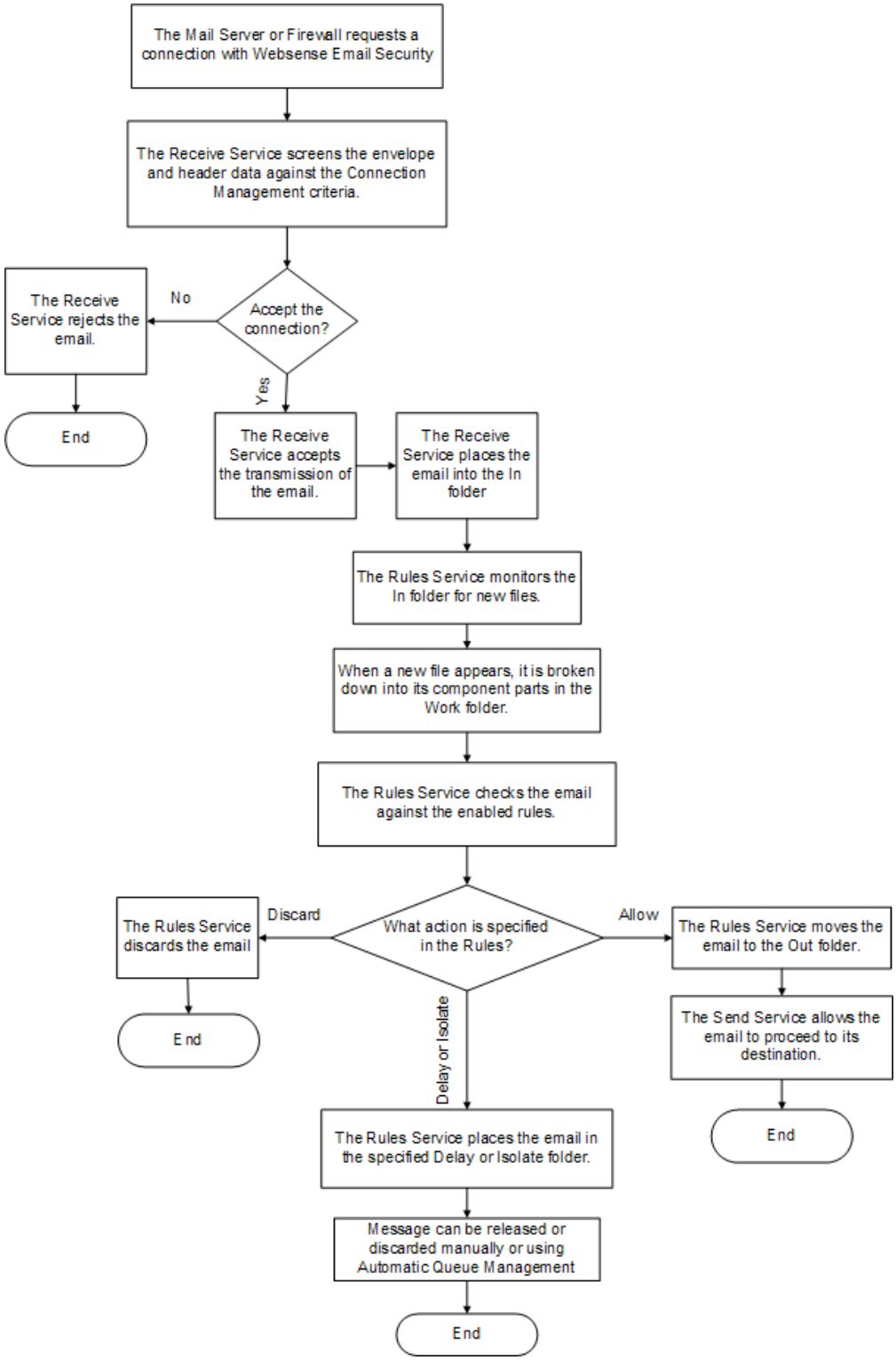
To display the version number of the Websense Email Security release installed on your system, right click on the Websense Email Security icon in the system tray and select **About**.

2 Finding Your Way Around Websense Email Security

To get the best utility and performance from Websense Email Security you should become familiar with:

How Websense Email Security works

This diagram shows how email is processed by Websense Email Security.

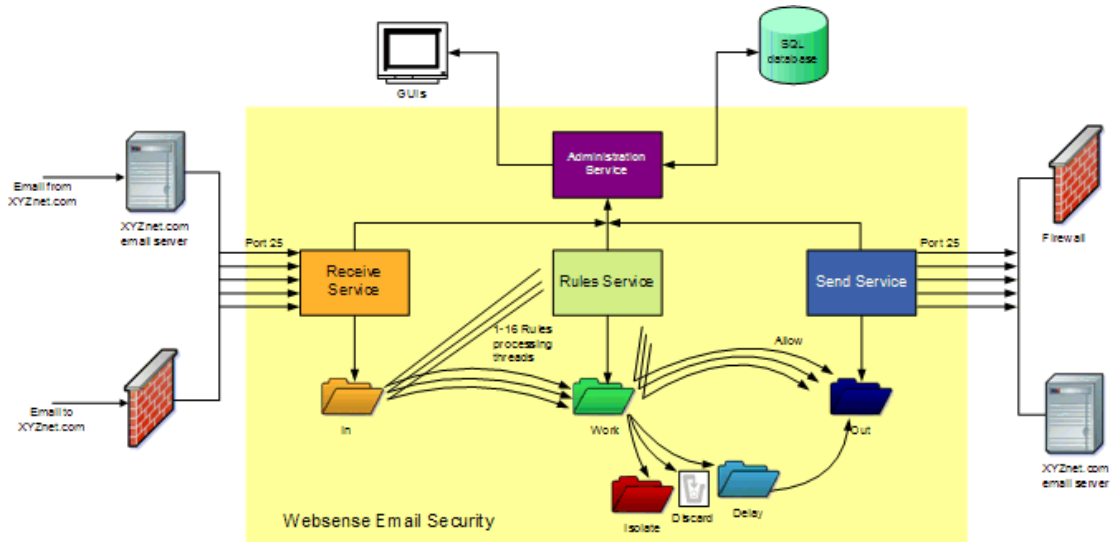


Websense Email Security services

Websense Email Security is managed by 4 software services:

- Receive Service: See *Configuring the Receive Service*, page 33.
- Rules Service: See *Configuring the Rules Service*, page 65.
- Send Service: See *Configuring the Send Service*, page 73.
- Administration Service: See *Configuring the Administration Service*, page 85.

The diagram below illustrates how the services fit together.



You can stop or start any of the services. See *Opening components from the system tray icon right-click menu*, page 25.

Websense Email Security components

The following 3 core components in Websense Email Security are used to manage email:

Component	Description
Monitor, page 98	The Monitor shows the progress of email in real-time as it moves through Websense Email Security. It also provides access to the Server Configuration console, the Rules Administrator, the Message Administrator, and other subcomponents.
The Rules Administrator, page 119	The Rules Administrator is used to set up email filtering rules to meet the needs of your Acceptable Use Policy (AUP).
Message Administrator, page 197	The Message Administrator is used to review, manage, and analyze email that has been placed in queues, and to view logs of Websense Email Security activity. You can also search for inbound and outbound email within predefined or custom date ranges.

Additional components

Websense Email Security includes the following additional components that enhance the capabilities of the core components.

Component	Description
Dashboard, page 109	The Dashboard provides an immediate visual picture of system health and activity.
QueueView, page 104	QueueView displays information about email that is queued, pending, or dead.
Dictionary Management, page 215	You can use dictionaries in rules to detect particular types of content in email, for example, adult, offensive, and so on. Use the Dictionary Management component to configure the supplied dictionaries or create and configure your own dictionaries.
Scheduler, page 227	Use the Scheduler to automate tasks such as: • Anti-Spam Agent, Internet Threat Database, Anti-Virus Agent, and Anti-Virus Malware Scanning updates. • Database maintenance • Queue synchronization

Component	Description
Web Administrator, page 241	The Web Administrator component enables you to access the following Websense Email Security functions from a remote computer: • Message Administrator • Dictionary Management • View logs
Virtual Learning Agent, page 253	The VLA enables you to train Websense Email Security to identify specific types of content in email, for example, confidential information that is specific to your organization.

Opening Websense Email Security components

There are several ways to open Websense Email Security components.

- *Opening components from the Start Menu*, page 25
- *Opening components from the system tray icon right-click menu*, page 25
- *Opening components from within other components*, page 26

Opening components from the Start Menu

Select **Start** > **Programs** (or **All Programs**) > **Websense Email Security** and select the desired component.

Selecting **Threat Database Manager** initiates an update of all enabled threat database components. Ordinarily, these updates are performed by tasks defined in the *Scheduler*, page 227.

Related topics

- *Opening components from the system tray icon right-click menu*, page 25
- *Opening components from within other components*, page 26

Opening components from the system tray icon right-click menu

When Websense Email Security is running, this icon is displayed in the system tray:

Right-click the icon to display a menu. Use the menu to open Websense Email Security components, configure the server, and stop and start the services.

Related topics

- *Opening components from the Start Menu*, page 25
- *Opening components from within other components*, page 26

Opening components from within other components

When a Websense Email Security component is open, you can open many other components from within that component. The icons of the available components are shown on the toolbar.

Icon	Component
	Dictionary Management
	Message Administrator
	Monitor
	Queue View
	Rules Administrator
	Scheduler
	Virtual Learning Agent (VLA)
	Web Administrator

Related topics

- *Opening components from the Start Menu*, page 25
- *Opening components from the system tray icon right-click menu*, page 25

The About box

You can view Websense Email Security version and subscription information from the Dashboard (in the Version panel) and by selecting **About** from the system-tray icon right-click menu, or in the Monitor by selecting **Help > About Websense Email Security**.

In the **About** box, click **Subscribe** to enter a subscription key. To get a key, click **Subscribe** and then click the link to **MyWebsense**.

For information about the Dashboard Version panel, see *Using the Version panel*, page 117.

3 Setting Up Websense Email Security

Setting up Websense Email Security consists of configuring Email Connection Management and the Receive, Rules, Send, and Administration services so that email is filtered correctly.

Connecting to a Websense Email Security server

Sites that use multiple Websense Email Security servers can select the server to connect to from any of several Websense Email Security components:

- *The Monitor*, page 97
- *Message Administrator*, page 197
- *The Rules Administrator*, page 119
- *Dictionary Management*, page 215

For example, you can view the email activity taking place on server A using an installation of Websense Email Security on server B. Server B can run either a full installation, or just the Websense Email Security Administration Client.

Related topics

- *Adding a Websense Email Security server*, page 29
- *Editing Websense Email Security server details*, page 30
- *Selecting a Websense Email Security server*, page 30
- *Disconnecting from a Websense Email Security server*, page 31

Adding a Websense Email Security server

To monitor email activity taking place on another server, add its connection details to the list of available servers.

To add a new server:

1. From any of the Websense Email Security components select **File > Select Server > Add New**. The **Add a New Server** dialog box displays.

2. In the **Server Name** field, enter or browse to the name of the server whose email traffic you want to monitor.
3. Enter the user name and password for accessing the server.
4. Enter the connection port for the mail server. This is the port used by the Administration Service.
5. Click **OK** to confirm your changes.

Websense Email Security automatically tries to monitor email activity on the server you added. If it fails to do this, check that you have entered the server details correctly.

Editing Websense Email Security server details

You can change the details of an email server on the server list.

To edit server details:

1. From any Websense Email Security component select **File > Select Server > Edit**. The **Select Server** dialog box appears.
2. Select the server to edit and click **OK**. The **Edit Server** dialog box appears.
3. Change the details as needed and click **OK**.

Note

You cannot change the server name.

Related topics

- *Connecting to a Websense Email Security server*, page 29
- *Adding a Websense Email Security server*, page 29
- *Selecting a Websense Email Security server*, page 30
- *Disconnecting from a Websense Email Security server*, page 31

Selecting a Websense Email Security server

Servers are listed on the **Select Server** drop-down menu.

1. From any Websense Email Security component select **File > Select Server**. The available servers are listed on the menu. The current server is indicated with a check mark.
2. Select the server to which you want to connect.
3. If the connection fails, check the server details.

Related topics

- *Editing Websense Email Security server details*, page 30
- *Connecting to a Websense Email Security server*, page 29
- *Adding a Websense Email Security server*, page 29
- *Disconnecting from a Websense Email Security server*, page 31

Disconnecting from a Websense Email Security server

To disconnect from the current server, select **File > Disconnect from Server**.

Email activity on that server is no longer displayed in the Monitor.

Related topics

- *Connecting to a Websense Email Security server*, page 29
- *Adding a Websense Email Security server*, page 29
- *Editing Websense Email Security server details*, page 30
- *Selecting a Websense Email Security server*, page 30

Opening the Server Configuration console

The Server Configuration console is used to configure the services.

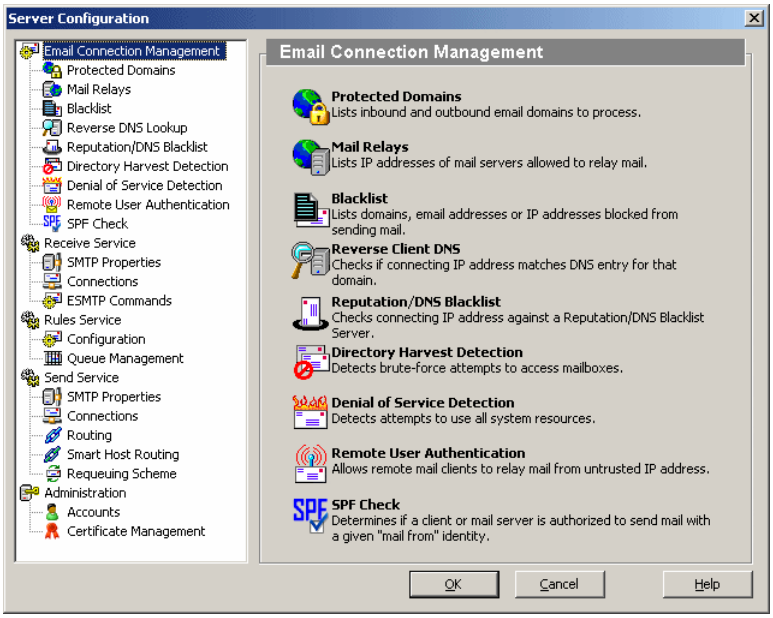
To open the Server Configuration console, on the Monitor toolbar, click 

Alternatively:

1. Open the Monitor and select **File > Server Configuration**.
2. In the left panel, navigate to the services and settings that you want to configure.

The Email Connection Management window:

Each function controls a group of Server Configuration settings



When you select a function, its settings display in the right panel of the console.

Related topics

- *Configuration workflow*, page 32
- *Configuring the Receive Service*, page 33
- *Configuring Connection Management*, page 39
- *Configuring the Rules Service*, page 65
- *Configuring the Send Service*, page 73
- *Configuring the Administration Service*, page 85

Configuration workflow

To set up Websense Email Security, you need to configure each service. Some services have more than 1 group of configuration settings in a series of dialog boxes. The table lists the functions in the Server Configuration console and where to find out more about each function.

Service	Function	Find out more
Receive Service	General Settings	*Receive Service - general settings*, page 34
	SMTP Properties	*SMTP properties*, page 35
	Connections	*Connections settings*, page 37
	ESMTP Commands	*ESMTP commands*, page 38

Service	Function	Find out more
Email Connection Management	Protected Domains	*Protected Domains*, page 39
	Mail Relays	*Mail Relays*, page 42
	Blacklist	*Blacklist*, page 51
	Reverse DNS Lookup	*Reverse DNS Lookup*, page 55
	Reputation/DNS Blacklist	*Reputation/DNS Blacklist*, page 57
	Directory Harvest Detection	*Directory Harvest Detection*, page 59
	Denial of Service Detection	*Denial of Service (DoS) detection*, page 62
	Remote User Authentication	*Remote User Authentication*, page 63
	SPF Check	*SPF Check*, page 64
Rules Service	General settings	*Rules Service general settings*, page 65
	Configuration	*Rules Service Configuration settings*, page 67
	Queue Management	*Queue management*, page 68
Send Service	General Settings	*Send Service - general settings*, page 73
	SMTP Properties	*SMTP properties*, page 74
	Connections	*Connections properties*, page 76
	Routing	*Routing*, page 77
	Smart Host Routing	*Smart Host routing*, page 82
	Requeuing scheme	*Requeuing*, page 84
Administration	Properties	*Administration settings - general*, page 86
	Accounts	*Configuring administrators for remote access*, page 87
	Certificate Management	*Certificate Management*, page 91

Configuring the Receive Service

The Receive Service accepts SMTP traffic on port 25 and checks each email against a series of Email Connection Management criteria. If the email passes those checks, Websense Email Security accepts the email and passes it to the Rules Service for further processing.

It is important to configure the Receive Service correctly to keep your email system running efficiently and securely, and to maintain the flow of legitimate email.

To configure the Receive Service, review and edit the following settings:

Receive Service - general settings

In the Server Configuration window select **Receive Service**.

Received mail drop-off folder

When an email has passed the Email Connection Management checks, Websense Email Security accepts the email and deposits it in the **Received mail drop-off folder** (the **\In** folder). The default path is:

```
C:\Program Files\Websense Email Security\In
```

To change the location, enter a different path or click **Browse** and select another location.

Enabling administrator alerts

The Dashboard hosts a robust alert system that includes queue size alerts. Use of that system is recommended. See *Using the Alerts panel*, page 111.

Independent of the Dashboard, you can elect to log a message in the Windows Event log when the number of pending messages in the **\In** folder exceeds a limit.

To enable administrator alerts:

1. In the Server Configuration console select **Queue Management**.
2. If you have already created your queue, select the queue and click **Edit**.

   If you need to add a queue, see *Adding a queue*, page 69.

   The **Queue Configuration** dialog box displays.
3. Select **Enable Administrator Alerts** and specify the number of messages the queue must contain before a message is logged (default = 1000).

Logging

The **Logging** options control where the details of email handled by the Receive Service are recorded. Select 1 or more check boxes for the required type of logging.

Logging option	What it does
Real-time console	Details of inbound messages are displayed in the Receive panel of the Monitor. For more information about the Monitor consoles, see *Service panels*, page 100.
System log	System events related to inbound mail, such as the sending of notification email, are displayed in the System log in Message Administrator. See *Working with logs*, page 212.
Connection log/Receive log	Information about connections from the host servers to Websense Email Security and about email that has been received by the Receive Service. This information is displayed in the Connection log and Receive log in Message Administrator. See *Working with logs*, page 212.

Related topics

- *Configuring the Receive Service*, page 33
- *SMTP properties*, page 35
- *Connections settings*, page 37
- *ESMTP commands*, page 38
- *Logs panel*, page 203

SMTP properties

Receive Service SMTP properties affect how Websense Email Security receives incoming email for filtering.

In the left panel, select **Receive Service > SMTP Properties**.

You can edit the following settings:

Field	Description
Receive Service SMTP Port	The port used by Websense Email Security to receive SMTP traffic. Change the port by entering a different port number here.
Enable Secure SMTP over SSL (SMTPS)	Select this to secure the entire SMTP conversation, that is, from connection to receiving the email, through secure connection over SSL (Secure Socket Layer). Default (recommended) port = 465 If this is selected and an SMTP port is specified, the sending clients must send email encrypted using SSL.

Field	Description
Computer Name	You can specify the computer name the Receive Service uses in its greeting when it receives a connection: • Windows Computer Name The Receive Service will use the fully-qualified primary domain name of the computer where Websense Email Security is installed. • Specify Computer Name The Receive Service will use the computer name you specify. You can use any commonly accepted form of host name, for example, the domain name or the IP address. By default, the Windows Computer Name is used.
SMTP greeting text	The SMTP greeting is the greeting sent to a remote computer when it initiates a connection by sending a HELO or EHLO command. By default, the SMTP greeting is: `220 [server name].[domain name]` If text is added, the SMTP greeting consists of the default text plus any additions. You can use the SMTP greeting text to communicate your organization's policy on how that mail server can be used. For example, if you do not allow the mail server to be used as a relay host, you can warn mail clients not to try to relay mail through your server. To change greeting. 1. Click **Customize**. The **Customize Greeting Text** dialog box displays. 2. Enter the Telnet SMTP greeting. This is displayed under the default greeting. 3. You cannot delete or edit the default greeting text. When a HELO or EHLO command is received, all the text visible in the box is sent as the greeting. 4. Click **OK** to close the Customize Greeting Text dialog.

Related topics

- *Configuring the Receive Service*, page 33
- *Receive Service - general settings*, page 34
- *Receive Service - general settings*, page 34

Connections settings

The Connections settings affect how many connections the Receive Service can accept, and how much incoming email it can process at any one time. It is important to set these limits to appropriate levels for your system's capacity.

To edit the Receive service **Connections** settings:

1. Open the Monitor and select **File > Server Configuration**. The **Server Configuration** console displays.
2. In the left panel, select **Receive Service > Connections**. The connection settings are displayed in the right panel.

The following table lists the connections you can limit. Select the check boxes corresponding to the limits you want to set. If a check box is cleared, Websense Email Security does not limit the number of connections.

Option	Description	Default	Maximum
Connection			
Maximum active Inbound connections	The total number of incoming connections that Websense Email Security will accept at any one time.	1500	9999
Limit maximum connections for each known IP address	Limit the number of connections Websense Email Security will accept from the IP addresses on the Trusted IPs List. See *Mail Relays*, page 42. If you set a limit here, the number must be less than or equal to the maximum number of active inbound connections.	1000	9999
Limit maximum connections for each unknown IP address	Limit the number of connections from IP addresses not on the trusted IP addresses list. If you set a limit here, the number must be less than or equal to the maximum number of active inbound connections.	100	9999
Idle connection timeout	Limits the number of seconds the Receive Service will wait to receive data before terminating the connection.	300	3600
Data size			
Limit maximum message size	Limit the size (in MB) of inbound email that Websense Email Security will accept.	20	500 MB
Limit maximum data per connection	Limit the total amount (in MB) of data that Websense Email Security will accept in a single connection.	70	700 MB

Option	Description	Default	Maximum
SMTP options			
Limit maximum messages per connection	Limit the total number of email that Websense Email Security will accept in a single connection.	10	100

Related topics

- *Configuring the Receive Service*, page 33
- *Receive Service - general settings*, page 34
- *SMTP properties*, page 35
- *ESMTP commands*, page 38

ESMTP commands

These options allow you to select the ESMTP commands to be used by the Receive Service in response to the SMTP EHLO command.

Select the check boxes of the commands to be used.

Option	Description
Authentication Options	
Enable AUTH-LOGIN	To enable or disable the ESMTP AUTH-LOGIN function
Enable AUTH-PLAIN	To enable or disable the ESMTP AUTH-PLAIN function
Enable AUTH-CRAM-MDS	To enable or disable the ESMTP AUTH-CRAM-MDS function
Transmission Optimizations	
Enable PIPELINING	Provides the ability to send a stream of commands without having to wait for a response after each command. This improves the speed of transmissions.
Enable CHUNKING	The size of each SMTP data chunk is sent with the data. This means that the SMTP host does not have to scan continuously for the end of the data. This improves the speed of transmissions.
Secure SMTP over TLS	
Enable STARTTLS	To enable a secure SMTP connection over Transport Layer Security (TLS)

The **Authentication Options** functions are used by remote users. To add details of remote users, see *Remote User Authentication*, page 63.

Related topics

- *Configuring the Receive Service*, page 33
- *Receive Service - general settings*, page 34
- *SMTP properties*, page 35
- *Connections settings*, page 37

Configuring Connection Management

You can add an extra layer of protection against unwanted email by setting up Email Connection Management. This means you can automatically drop connections from untrustworthy sources and control incoming email before messages are filtered.

Email Connection Management has these functions:

- *Protected Domains*, page 39
- *Mail Relays*, page 42
- *Blacklist*, page 51
- *Reverse DNS Lookup*, page 55
- *Reputation/DNS Blacklist*, page 57
- *Directory Harvest Detection*, page 59
- *Denial of Service (DoS) detection*, page 62
- *Remote User Authentication*, page 63
- *SPF Check*, page 64

Protected Domains

Use Protected Domains to identify the domains for which email is to be filtered, and for which Websense Email Security will accept email. When Websense Email Security was installed, a primary domain name was established, however, if your network has more than 1 domain, for example mycompany.co.uk and mycompany.com, you must enter the other domains so that they can send and receive email.

Note

There must always be at least 1 domain in the Protected Domains list.

Warning

Do not add a protected domain to the blacklist. Websense Email Security does not check the Protected Domains list for duplicate entries on the Blacklist. If protected domains are added to the Blacklist, email to the protected domain is rejected.

Related topics

- *Adding Protected Domains*, page 40
- *Editing a Protected Domain*, page 40
- *Deleting a Protected Domain*, page 41
- *Anti-Spoofing*, page 41
- *Anti-relay protection*, page 42

Adding Protected Domains

To add a protected domain:

1. Open the Monitor and select **File > Server Configuration**.
2. In the Server Configuration console select

   Email Connection Management > Protected Domains.

   The **Protected Domains** dialog box displays.
3. Click **Add**. The **Protected Domain Properties** dialog box displays.
4. In the **Domain name** field, enter the name of the domain for which you want Websense Email Security to accept email. For example:

   `mycompany.co.uk`

   The **Administrator email address** field is filled in automatically as Postmaster@ the domain you specify, for example, Postmaster@mycompany.co.uk.

   You can edit this address. For example, you could change it to admin@mycompany.co.uk
5. Click **OK**.

Editing a Protected Domain

To edit a protected domain:

1. Open the Monitor and select **File > Server Configuration**.
2. In the Server Configuration console select

   Email Connection Management > Protected Domains.
3. In the **Protected Domains** dialog box, select the domain to change.
4. Click **Edit**. The **Protected Domain Properties** dialog box displays.

5. Change the domain name or the administrator's email address as needed.
6. Click **OK**.

Deleting a Protected Domain

You can also delete a domain from the Protected Domains list so that Websense Email Security no longer accepts email for that domain.

To delete a protected domain:

1. Open the Monitor and select **File > Server Configuration**.
2. In the Server Configuration console select

   Email Connection Management > Protected Domains.
3. In the **Protected Domains** dialog box, select the domain to change.
4. Click **Delete** and confirm your choice.
5. Click **OK**. The domain is removed from the list and Websense Email Security no longer accepts email for that domain.

Anti-Spoofing

Spammers sometimes use a technique called "spoofing" to fake their **From** address so that their email appears to be from a protected domain.

By default, anti-spoofing and *Anti-relay protection* are enabled.

Warning

Disabling Anti-Spoofing makes it possible for spammers to send spoofed email into your organization. By default, Anti-Spoofing is enabled. It is recommended that you keep it enabled.

To change the settings, see *Changing Anti-Spoof and Anti-Relay settings*.

When Anti-Spoofing is enabled, Websense Email Security examines and authenticates the IP address of all incoming email and rejects email that cannot be authenticated. If you do not enable this function, email from the protected domains is accepted without examining the From address.

If your organization includes users who send mail from the protected domain from an unlisted IP address, for example dial-up users, you should set up Websense Email Security to authenticate addresses using **Receive Service Remote User Authentication**. This allows legitimate email from these users to get through, while still denying email from fraudulent addresses.

See *Remote User Authentication*, page 63 for information about how to set up remote users.

Anti-relay protection

Spammers may attempt to relay email through your email server using old routing techniques. These routing techniques are not commonly used any more but may still be recognized by your mail server.

Websense Email Security detects various routing relay techniques and denies email that has been forwarded or routed using one of the following routing methods.

Relay method	Example
Bang routing	`domain2!domain1!user@domain.com`
Quoted routing	`"user@domain1.com"@domain.com`
Source routing	`@domain1.com:user@domain.com`
Percent hack routing	`user%@domain1.com@domain.com`

If you do not deny Source routing, Websense Email Security strips any additional routing information from the incoming email, so an email from:

`@hotmail.com:user@company.com`

is delivered as:

`user@company.com`

Changing Anti-Spoof and Anti-Relay settings

1. In the Server Configuration console select

   Email Connection Management > **Protected Domains**.
2. Click **Advanced**. The **Anti-Spoof settings** dialog box appears.
3. By default, all anti-spoofing and anti-relay protection options are enabled. To disable an option, clear the check box.

   Websense recommends you keep all options selected to protect your system.
4. Click **OK**.

Mail Relays

Mail Relays are the IP addresses of mail servers that are allowed to send email to and from the protected domain. You should include details of all the mail servers for which you want to filter email.

The purpose of this list is to identify:

- The IP addresses of the protected domains
- The IP addresses of any other nodes that need to access the protected domains from outside the network

When you add or edit a Mail Relay, you need to specify what email can be relayed through that server by choosing a relay type, and also whether email received from

this IP address must be through an encrypted connection. You can select from the following options.

Option	Description
Trusted mail relay	The mail relay is trusted. Connection management is not applied to trusted mail relays.
Outbound	The mail relay can send email only to IP addresses outside the protected domain. The message sender must be in the protected domain, be a non-delivery receipt (NDR), or be from a null sender address (< >). The message recipient must be outside the protected domain.
Inbound	The mail relay can send email only to IP addresses inside the protected domain. The message sender must be outside the protected domain. The message recipient must be inside the protected domain.
Outbound and inbound	The mail relay is allowed to send email to any IP address, except those on the blacklist. The message sender can be inside or outside the protected domain. The message recipient can be inside or outside the protected domain. One, either the sender or the recipient, must be inside the protected domain.
Open relay	The mail relay is allowed to send email to any other domain, including blacklisted domains, without any relay restrictions. Websense Email Security accepts any email from the supplied IP address regardless of the domain name. **Warning:** Use with caution.
Email received from this IP address must be via an encrypted connection	Default = Cleared If selected, the sending mail server for this relay must send encrypted email to the Receive Service using STARTTLS. If the mail server does not support TLS, the connection is dropped. **Note:** If selected, this overrides the Enable STARTTLS option in the ESMTP Commands dialog box. See *ESMTP commands*, page 38.

Allow connections from other direct relays

By default, Websense Email Security accepts connections from unlisted direct relays.

To limit connections to *only* listed mail relays, uncheck **Allow connections from other direct relays**.

If connections are allowed from other direct relays (the default), you can specify a list of domains that must use a secure TLS connection. See *Specifying domains that require an encrypted connection*, page 48.

Related topics

- *Adding a Mail Relay*, page 45
- *Importing Mail Relays*, page 46
- *Editing a Mail Relay*, page 47
- *Deleting a Mail Relay*, page 47
- *ESMTP commands*, page 38

Trusted mail relay

Identifies the mail relay as trusted. Connection management is not applied to trusted mail relays.

Outbound

The mail relay can send email *only* to IP addresses outside the protected domain.

The message sender must be in the protected domain.

The message recipient must be outside the protected domain.

Inbound

The mail relay can send email *only* to IP addresses inside the protected domain.

The message sender must be outside the protected domain.

The message recipient must be inside the protected domain.

Outbound and inbound

The mail relay can send email to any IP address, except those on the blacklist.

The message sender can be inside or outside the protected domain.

The message recipient can be inside or outside the protected domain.

One, either the sender or the recipient, must be inside the protected domain.

Open relay

Use with caution.

The mail relay is allowed to send email to any other domain, including blacklisted domains, without any relay restrictions. Websense Email Security accepts email from the supplied IP address regardless of the domain name.

Email from this IP must be on an encrypted connection

Default = Cleared

If this option is selected, the sending mail server from this relay must send encrypted email to the Receive Service using STARTTLS. If the mail server does not support TLS, the connection is dropped.

> **Note**
> If selected, this option overrides the **Enable STARTTLS** option in the **ESMTP Commands** dialog box. See *ESMTP commands*, page 38.

Adding a Mail Relay

To add a mail relay, you must:

- Define the direct mail relays – These mail relays communicate directly with Websense Email Security using SMTP, both inside and outside the network perimeter.
- Define the outlying mail relays – These mail relays exist within the network perimeter, but do not communicate directly with Websense Email Security using SMTP. These relays cannot be marked as trusted, but are treated as such when determining True Source IP.

Defining direct Mail Relays:

1. In the Server Configuration console, select

   Email Connection Management > Mail Relays > Direct tab.
2. Click **Add**. The **Connected Mail Relay Properties** dialog box appears.
3. Enter the server IP address, or a range of server IP addresses, for which you want email to be filtered.

   If you enter a range of IP addresses, it must be in Classless Inter-Domain Routing (CIDR) format. For example, for a 24-bit mask:

   Correct:

   `200.0.0.1/24`

   Incorrect:

   `200.0.0.1-200.0.0.255`
4. You can also enter a description for the mail relay. This name is shown in the hostname field of the logging database (LogDB) and is useful for identifying the mail server in reports.
5. Select a relay type and whether the email should be sent on an encrypted connection. See *Mail Relays*, page 42 for more information.

6. Click **OK**.

> **Note**
> You cannot enter the same IP address twice. If you enter an IP address that is already listed, the following message is displayed:
> `"Duplicate entry, please try again."`

Defining outlying Mail Relays:

1. In the Server Configuration console, select

   Email Connection Management > **Mail Relays** > **Outlying** tab.
2. Click **Add**. The **Outlying Mail Relay Properties** dialog box appears.
3. Enter the server IP address or a range of addresses for which you want email to be filtered.

   If you enter a range of IP addresses, it must be in CIDR format. For example, for a 24-bit mask:

   Correct:

   `200.0.0.1/24`

   Incorrect:

   `200.0.0.1-200.0.0.255`
4. You can also enter a description for the mail relay. This name is shown in the hostname field of the logging database (LogDB) and is useful for identifying the mail server in reports.
5. Click **OK**.

> **Note**
> You cannot enter the same IP address twice. If you enter an IP address that is already listed, the following message is displayed:
> `"Duplicate entry, please try again."`

Importing Mail Relays

When you want to import an IP address or range of addresses for mail relays, the data in the file must have the following format:

<ip address range>;<description>;<type>;<encrypted>[;<untrusted>]

- IP address range – Either a single IP address or a range of addresses in CIDR format
- Description – Cannot include a semicolon (;)
- Type – A number that represents the type of connection:

Valid “Direct” connection types

- 0 = Outbound
- 1 = Inbound
- 2 = Outbound/Inbound
- 3 = Open

Valid “Outlying” connection type

- 4 = Outlying

- Encrypted – “yes” or “no”
- Untrusted – For a trusted connection you can leave this field empty, or enter “no”. For an untrusted connection you must enter “yes”.

  Examples of correct formats:

  192.168.1.5;inbound;1;yes;yes

  192.168.1.4;outbound;0;yes

  192.168.1.2;open relay; 3; no

  192.168.1.1;outlying;4;yes

  192.168.1.10/24;outbound/inbound;2;yes

To import the details of mail relays:

1. In the Server Configuration console, select **Email Connection Management > Mail Relays**.
2. Select either the **Direct** tab or the **Outlying** tab.
3. Click **Import**.
4. Select the text (.txt) file and click **Open**.

The entries are added to the list.

Editing a Mail Relay

To edit the details of a mail relay:

1. In the Server Configuration console select **Email Connection Management > Mail Relays**.
2. Select the IP address to edit.
3. Click **Edit**. The **Edit Relay Source** dialog box appears.
4. Change the options as required and click **OK**.

Deleting a Mail Relay

To delete a mail relay:

1. In the Server Configuration console select **Email Connection Management > Mail Relays**.
2. Select the IP address to delete and click **Delete**.

3. You are prompted to confirm your choice. Click **Yes** to delete the IP address.

Specifying domains that require an encrypted connection

If **Allow connections from other direct relays** is enabled (the default), you can create a list of domains that must use an encrypted connection (TLS).

Click **Add** to add a domain to the list. The **Domain Properties** dialog box displays. Enter a domain name and, optionally, a description.

Click **Edit** to change an existing entry. The **Domain Properties** dialog box displays. Change the domain name or description.

To delete an entry, select the domain from the list and click **Delete**.

The same domain cannot be listed twice, nor is a subdomain of a listed domain allowed.

Receive Service Status Messages

When a mail client attempts to connect to Websense Email Security, a status message is displayed in the Receive panel of the Monitor.

Common status messages and examples include:

Message	Description
The sender must be from a protected domain as its IP is in the Trusted Outbound list.	The mail client's IP address has been added to the Trusted IPs list with a setting of **Outbound.** The Receive Service has rejected the connection because the sender is not in the protected domain.
The recipient must not be to a protected domain as the sender's IP is in the Trusted Outbound list.	The mail client's IP address has been added to the Trusted IPs list with a setting of **Outbound.** The Receive Service has rejected the connection because the recipient is inside the protected domain.
The sender must not be from a protected domain as the sender's IP is in the Trusted Inbound list.	The mail client's IP address has been added to the Trusted IPs list with a setting of **Inbound**. The Receive Service has rejected the connection because the sender is inside the protected domain, or is spoofed to appear to be from inside the protected domain.
The recipient must be to a protected domain as the sender's IP is in the trusted Inbound list.	The mail client's IP address has been added to the Trusted IPs list with a setting of **Inbound**. The Receive Service has rejected the connection because the sender has attempted to send an email to an IP address outside the protected domain.
Connection rejected – deny connection for unknown [n.n.n.n] (sender in Deny Connection list).	The IP address has been added to the Blacklist. The mail client is prohibited from making a connection to the Receive Service.

True Source IP Detection

The True Source IP Detection feature allows the connection management features of Websense Email Security to be used effectively, even if it is downstream from a firewall or an internal mail relay. Instead of using the IP of the connecting upstream MTA, the information in the message header is used to determine the IP address of the first sender outside the network perimeter. See Example 1 and Example 2 below.

Where it is Used

This IP address is used when applying the following Email Connection Management techniques:

- *Blacklist*, page 51
- *Reputation/DNS Blacklist*, page 57
- *Directory Harvest Detection*, page 59
- *SPF Check*, page 64

Configuring True Source IP Detection

There are two steps to configuring Websense Email Security to use True Source IP Detection:

1. Define the **Direct Mail Relays**. These are mail relays that communicate directly to the Websense Email Security through SMTP from both inside and outside the network perimeter.

   There are three type of Direct Mail Relays:

   - **Trusted** – Any SMTP conversation from an IP address or IP address range that is defined in the Direct Mail Relays list to be trusted will not have connection management applied.

     Connections of this type should be used when the connecting mail relay is well known and trusted. For example, for outbound connections from internal mail servers or for inbound connections from mail servers run by trusted parties.

   - **Untrusted** – Any SMTP conversation from an IP address or IP address range that is defined in the Direct Mail Relays list and *not* set to be trusted will have connection management applied using the IP address determined from the True Source IP Detection (instead of the connecting IP Address). Other connection management such as Directory Harvest Detection can also be applied to these connections. Connections of this type should be used for internal mail relays and store and forward firewalls.

   - **Unknown** – Any SMTP conversation from an IP address or IP address range not defined in the Direct Mail Relays list will have connection management applied using the IP address of the connecting server. However, if the **Allow connections from other direct relays** check box is not selected, the connection will be denied.

2. **Define the Outlying Mail Relays**. These are relays that exist within the network perimeter but do not communicate directly to Websense Email Security via SMTP. These relays cannot be marked as trusted but in essence when determining the True Source IP they are treated that way.

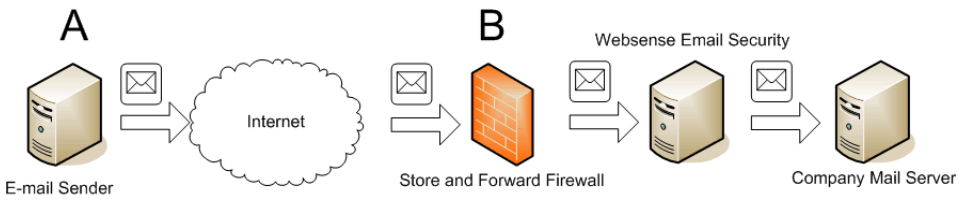
Example 1 — Network with Firewall

For an environment using a firewall but no mail relay, the 2 steps to configure the mail relays to enable Email Connection Management to be used for email from sender A to the company mail server are:

1. Set Direct Mail Relays:
   a. Set up B (store and forward firewall) as an non trusted Direct Mail Relay in the Inbound direction.
   b. Set up Company Mail Server as a trusted direct connection in the outbound direction
2. Set Outlying Mail Relays:

   None

This applies connection management using the IP Address of A—or any other external connection coming inbound through the firewall—but does not apply connection management outbound for the company mail server because this is trusted.



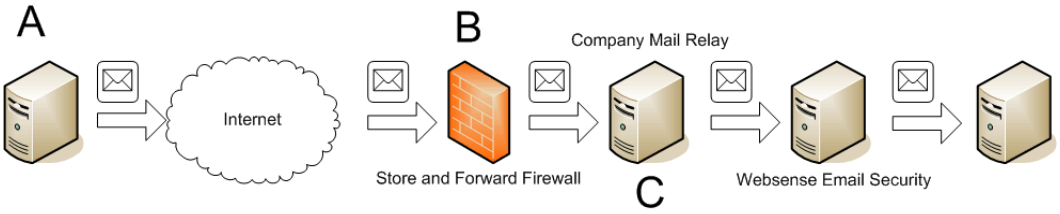
Example 2 — Network with Firewall and Mail Relay

For an environment using a firewall and a mail relay, the 2 steps to configure the mail relays to enable Email Connection Management to be used for email from sender A to the company mail server are:

1. Set Direct Mail Relays:
   a. Set up C (Company Mail Relay) as an “untrusted” Direct Mail Relay in the Inbound direction.
   b. Set up Company Mail Server as a trusted direct connection in the Outbound direction.
2. Set Outlying Mail Relays:

   Set up B (store and forward firewall) as an Outlying Mail Relay as it does not communicate directly with the Websense Email Security but does forward mail to it.

This applies connection management using the IP Address of A—or any other external connection coming inbound via the firewall—but does not apply connection management outbound for the Company Mail Server because it is trusted.



Blacklist

If there are domains, email addresses or IP addresses from which you do not want to receive email, you can add them to the Blacklist. This is an important step in preventing unwanted email content because:

- The Receive Service will reject the email before the email content is transferred to your mail server
- No hard disk space is wasted storing unwanted email
- Fewer messages have to be processed by the Rules Service, which conserves system resources

When an email has been added to the Blacklist, an “Update Now” message is displayed in the Monitor. If you click **Yes**, a status message “Receive service configuration reloaded” is displayed in the Receive panel of the Monitor.

The Receive Service rejects any mail client that tries to send email from any of the set domains, email addresses or IP addresses, unless the mail client’s IP is added to the Trusted IP list with a setting of Open Relay.

Warning
Do not add the protected domain to the Blacklist, or email to the protected domain will be rejected.

If you have added a domain to the Blacklist, but want Websense Email Security to accept email from individuals within that domain, you can exclude individuals from the blacklist.

Related topics

- *Adding an item to the Blacklist*, page 52
- *Excluding an item from the Blacklist*, page 53
- *Editing an item on the Exclude List*, page 53
- *Importing a Blacklist*, page 54
- *Mail Relays*, page 42

Adding an item to the Blacklist

To add an item to the Blacklist:

1. In the Server Configuration console select

   Email Connection Management > Blacklist.

2. Click **Add**. The **Add/Edit deny list entry** dialog box displays.

> **Note**
> Text boxes are limited to 255 characters.

3. Enter the domain, email address or IP address to be blacklisted. In the **Comment** field enter a brief description of the item, or an explanation of why it is blacklisted.

   You can blacklist an entire range of IP addresses by entering only the first 3 number sets in the IP address. For example, to blacklist all IPs from 172.22.5.0 to 172.22.5.255, you could add 172.22.5 to the Blacklist.

> **Note**
> You cannot blacklist a partial range of numbers, for example IPs from 172.22.5.10 – 172.22.5.25.

4. Click **OK**. The Blacklisted items are displayed in the list.

When an email has been added to the Blacklist, an “Update Now” message is displayed in the Monitor. If you click **Yes**, a status message “Receive service configuration reloaded” is displayed in the Receive panel of the Monitor.

The Receive Service will reject any mail client trying to send an email from any of the set domains, email addresses or IP addresses, unless the mail client’s IP is added to the Trusted IP list with a setting of Open Relay.

> **Warning**
> Do not add the protected domain to the Blacklist, or email to the protected domain will be rejected.

If you have added a domain to the Blacklist, but want Websense Email Security to accept email from individuals within that domain, you can exclude individuals from the Blacklist. For example, if your organization was pursuing a grievance with another organization, you might want to block all email from that organization except for their legal department.

Related topics

- *Blacklist*, page 51
- *Excluding an item from the Blacklist*, page 53
- *Editing an item on the Exclude List*, page 53
- *Importing a Blacklist*, page 54
- *Mail Relays*, page 42

Excluding an item from the Blacklist

To exclude an item from the Blacklist:

1. In the Server Configuration console select
   Email Connection Management > Blacklist.
2. Click **Exclude**. The **Exclusions from the Blacklist** dialog box displays.
3. Click **Add**. The **Exclusions List Entry** dialog box displays.
4. Enter the email address to exclude from the Blacklist.
   You can specify that the address is for a Sender, Receiver, or Both.

   Note
   The email address must have fewer than 255 characters.

5. Click **OK**.

Related topics

- *Blacklist*, page 51
- *Adding an item to the Blacklist*, page 52
- *Editing an item on the Exclude List*, page 53
- *Importing a Blacklist*, page 54

Editing an item on the Exclude List

To edit an item on the Exclude list:

1. In the Server Configuration console select
   Email Connection Management > Blacklist.
2. Click **Exclude**. The **Exclusions from the Blacklist** dialog box displays.
3. Select the item to edit, and then click **Edit**. The **SMTP List Entry** dialog box displays.
4. Make your changes and click **OK**.

Related topics

- *Blacklist*, page 51
- *Adding an item to the Blacklist*, page 52
- *Excluding an item from the Blacklist*, page 53
- *Importing a Blacklist*, page 54

Deleting an item from the Exclude List

To delete an item from the Exclude list:

1. In the Server Configuration console select

   Email Connection Management > Blacklist.
2. Click **Exclude**. The **Exclusions from the Blacklist** dialog box displays.
3. Click **Delete**. You are prompted to confirm your choice.
4. Click **Yes** to delete the item. Websense Email Security will no longer accept email from this domain, email address or IP address.

Importing a Blacklist

If there are a large number of domains, email addresses or IP addresses that you want to blacklist or exclude, you can create a text file listing all of the items, and import it into Websense Email Security. The text file can contain the items to blacklist, and the items to be excluded from the Blacklist.

There are 2 parts to this process, creating the list and importing it.

Create a text file with the blacklist items:

1. Create a new .txt file with any text editor.
2. In the .txt file, enter the domains, email addresses or IP addresses to be blacklisted. Each item in the list must have this format:

   `type;domain, email address or IP address;comment`

   Each list item must begin on a new line.

   If you do not want to add a comment, leave a blank after the final semicolon.

   “type” is a numerical code to identify whether the item is a domain, an email address or an IP address:

   0 = domain

   1 = email address

   2 = email address to be excluded from the Blacklist

   3 = IP address.

   Examples:

   0;yahoo.co.uk;internet mail

1;mailinglist.org.uk; known spammer

2;legitimatemail@mailinglist.org.uk; legitimate newsletter.

3. When the list is complete, save it to a location that is accessible to the Websense Email Security server. Saving it in the **Websense Email Security** folder will save time because the import facility looks there first.

Import the blacklist text file:

1. In the Server Configuration console select

   Email Connection Management > Blacklist.
2. Select **Import**.
3. Select the blacklist file and click **Open**.

If the blacklist file imports successfully, a confirmation message is displayed and the blacklisted domains, email addresses and IP addresses are displayed in the list.

If the file does not import successfully, check that every entry has the correct syntax.

Related topics

- *Blacklist*, page 51
- *Adding an item to the Blacklist*, page 52
- *Excluding an item from the Blacklist*, page 53
- *Editing an item on the Exclude List*, page 53

Reverse DNS Lookup

The Receive Service can check that an email is from a legitimate source by verifying that the domain name specified by the sending mail client in the HELO/EHLO greeting matches the domain name in its DNS record:

1. When a mail client requests a connection to the Receive Service, the Receive Service performs a reverse DNS lookup on that client's IP address to receive its PTR record. The default timeout is usually 3 seconds.
2. If the PTR record does not exist, or if the DNS record doesn't match the host name specified in the HELO/EHLO command, the Receive Service terminates the connection at the MAIL FROM command, unless the sending mail client authenticates itself.

If a mismatch is detected, there are 3 actions Websense Email Security can take.

Action	What it does
Log Only	The mismatch of domain names is displayed in the Receive Service panel of the Monitor, but the Receive Service accepts the connection and continues to process the email.
No DNS record found	If the Receive Service cannot find a DNS record that corresponds to the IP address of the sending mail server, and the sending mail client fails to authenticate itself, the connection is terminated at the MAIL FROM command.
DNS record fails to match HELO string.	If the domain name in the DNS record does not match the one in the HELO/EHLO command, the Receive Service terminates the connection at the MAIL FROM command, unless the sending mail client authenticates itself.

Enabling Reverse DNS Lookup, page 56

Excluding a mail server from Reverse DNS Lookup, page 56

Enabling Reverse DNS Lookup

By default, Reverse DNS Lookup is not enabled:

1. In the Server Configuration console select the **Reverse DNS Lookup** function.
2. Select **Enable Reverse DNS lookup**.
3. Select the action Websense Email Security will take if the domain names in the HELO string and the DNS record do not match.

Excluding a mail server from Reverse DNS Lookup

It is an RFC recommendation, but not a requirement, that the HELO/EHLO command contain the fully-qualified domain name (FQDN) of the sending mail client. If you have chosen to deny the connection, you may find that legitimate email is blocked because the sending mail client does not use the FQDN in its HELO/EHLO command. To avoid blocking legitimate email you should either:

- Select to only log the mismatch.
- Exclude any known legitimate servers that may have a mismatched DNS/HELO string.

To exclude a mail server from Reverse DNS Lookup:

1. In the Server Configuration console select the **Reverse DNS Lookup** function.
2. Click **Exclude**. The **Exclusion from Client DNS Lookup** dialog box displays.
3. Click **Add**. The **SMTP List Entry** dialog box displays.
4. Enter the IP address you want to exclude from Reverse DNS Lookup.
5. Click **OK**.

Reputation/DNS Blacklist

Websense Email Security can check an email sender's True Source IP address against the Websense ThreatSeeker Reputation Service, or a list of spammers held on 1 or more DNS Blacklist servers (you provide the domain name of the DNS Blacklist servers).

Related topics

- *Checking IP addresses against the Websense Reputation Service*, page 57
- *Checking IP addresses against DNS Blacklist servers*, page 57
- *Actions for Reputation/DNS Blacklist checking*, page 59
- *Excluding mail servers from Reputation/DNS Blacklist checking*, page 58

Checking IP addresses against the Websense Reputation Service

To use the Websense Reputation Service, simply select **Activate Websense Reputation Service**.

In the event that Websense changes the URL of the Reputation service, you will have to change server address.

1. Click **Configure**. The **Reputation Service Customer ID** dialog box displays.
2. Click **Edit**, change the address, and click **OK**.

Warning

Do not click **Regenerate** unless specifically instructed to do so by Websense Technical Support.

Related topics

- *Checking IP addresses against DNS Blacklist servers*, page 57
- *Actions for Reputation/DNS Blacklist checking*, page 59
- *Excluding mail servers from Reputation/DNS Blacklist checking*, page 58
- *Reputation/DNS Blacklist*, page 57

Checking IP addresses against DNS Blacklist servers

To use a 3rd party DNS Blacklist server to check the reputation of the inbound IP address, select **Check IP addresses against DNS Blacklist servers**.

1. Select **Activate Websense Reputation Service** to use the Websense Reputation service.

2. Select **Check IP addresses against DNS Blacklist servers** to use a 3rd party DNS Blacklist server.
3. Click **Add** to specify a DNS Blacklist server. The **SMTP List Entry** dialog box displays.
4. Enter the domain name of the DNS Blacklist server to use and click **OK**. The server is displayed in the **DNS Blacklist Servers** list.

Related topics

- *Checking IP addresses against the Websense Reputation Service*, page 57
- *Actions for Reputation/DNS Blacklist checking*, page 59
- *Excluding mail servers from Reputation/DNS Blacklist checking*, page 58
- *Reputation/DNS Blacklist*, page 57

Excluding mail servers from Reputation/DNS Blacklist checking

A legitimate organization can sometimes be wrongly placed on a Reputation DNS Blacklist server, for example if its domain name has been used by a spammer to send spoofed email. You can exclude legitimate IP addresses from Reputation DNS Blacklist server lookups, so that Websense Email Security will accept email from those sources. If any email you receive is mission-critical, you should make sure the sender's IP address is excluded from being checked against a DNS blacklist or the Websense Reputation service.

To exclude a mail server from Reputation DNS Blacklist server lookups:

1. In the Server Configuration console select

   Email Connection Management > Reputation/DNS Blacklist.
2. Select **Exclude**. The **Exclusions** dialog box displays.
3. Click **Add**. The **SMTP List Entry** dialog box displays.
4. Enter the IP address to exclude from Reputation DNS Blacklist lookups. If you have set up reverse DNS lookup for a domain, you can enter that domain. Websense Email Security will then accept connections from this source. See *Reverse DNS Lookup*, page 55.
5. Click **OK**.

Related topics

- *Checking IP addresses against DNS Blacklist servers*, page 57
- *Actions for Reputation/DNS Blacklist checking*, page 59
- *Actions for Reputation/DNS Blacklist checking*, page 59
- *Reputation/DNS Blacklist*, page 57

Actions for Reputation/DNS Blacklist checking

In the **Action** section of the **Reputation DNS Blacklist** screen, select how you want Websense Email Security to deal with a connection from a sender's IP address that comes back positive from the Websense Reputation Service or DNS blacklist:

- **Log Only** – Information about the connection is recorded in the Connection log and displayed in the Monitor.
- **Deny connection** – The connection is dropped and email from that sender is rejected.

Related topics

- *Checking IP addresses against DNS Blacklist servers*, page 57
- *Checking IP addresses against the Websense Reputation Service*, page 57
- *Excluding mail servers from Reputation/DNS Blacklist checking*, page 58
- *Reputation/DNS Blacklist*, page 57

Directory Harvest Detection

Spammers use a variety of methods to "mine" your organization for valid email addresses. When they succeed, it not only causes an increase in spam, but also slows down the delivery of legitimate email.

A common technique is to flood a mail server with a large number of messages using fabricated email addresses. The addresses that are not immediately rejected by your mail server are assumed to be valid and are added to the spammer's database of valid addresses.

Websense Email Security can detect when a server is trying to send large numbers of messages for the purposes of directory harvesting, by keeping a count of:

- The number of invalid email addresses or domains per connection
- The number of invalid email addresses or domains from each IP address per hour

Note

If you restart the Receive Service, these counts are reset to zero.

You can configure the Receive Service to terminate a connection when these counts reach a threshold.

Directory Harvest Detection (DHD) uses Lightweight Directory Access Protocol (LDAP) to check the validity of email addresses and domains. LDAP is an Internet protocol that email and other programs use to look up information from a server. To use Directory Harvest Detection, you must configure one or more LDAP connections.

Domain Substitution

You can use Domain Substitution if your recipient address could be in one of several domains but your LDAP server is only configured with the primary domain. This feature enables you to configure a list of alternative domains so that if an alternative domain is in the “Recipient” field and LDAP is enabled, the LDAP lookup uses the primary domain for the lookup. Example:

jane.mann@myco.com = primary domain

jane.mann@myco_uk.com = alternative domain

jane.mann@myco_us.com = alternative domain

This feature is used so that messages to the alternative domains do not trigger the Directory Harvest Detection feature. When LDAP is enabled, the information is also used in the *From Users and Groups object* and the *To Users and Groups object* for lookups of the “To” address.

Related topics

- *Enabling Directory Harvest Detection*, page 60
- *Enabling Domain Substitution*, page 62
- *From Users and Groups object*, page 142
- *To Users and Groups object*, page 144

Enabling Directory Harvest Detection

To enable Directory Harvest Detection:

1. Open the Server Configuration console and select
   Email Connection Management > Directory Harvest Detection.
2. Check **Enable Directory Harvest Detection**.
3. Configure the LDAP connection. Use of LDAP is required. See *Configuring the LDAP server*, page 61.
4. Optionally, enable domain substitution. See *Enabling Domain Substitution*, page 62.
5. Optionally, exclude trusted servers. See *Excluding legitimate email addresses or domains*, page 62.
6. Set **Maximum invalid addresses per connection** to the desired threshold.
7. Set **Maximum invalid addresses from each IP per hour** to the desired threshold.
8. Select an action to take when a threshold is exceeded.
   - Select **Log only** to *only* log the condition.
   - To deny the connection, select **Deny connection from IP** and set the number of hours the connection is to be denied.

If True Source IP Detection is *not* enabled and a threshold is exceeded, the connection is denied regardless of the **Action taken** setting. (True Source IP Detection is highly recommended. See *True Source IP Detection*, page 49.)

If True Source IP Detection is enabled and **Deny connection from IP** is selected, when a Directory Harvest Detection threshold is exceeded, the True Source IP address of the connection is blacklisted for the specified period.

Note

Until a threshold is exceeded, connections from the IP are accepted.

Configuring the LDAP server

1. Click **LDAP** to configure and manage your LDAP servers and connections.

   The **LDAP Connections** dialog box displays. You can configure 1 or more LDAP connections.

2. If there are no connections in the list, or if you want to add more connections, click **Add**.
3. The **Add LDAP Connection** dialog box displays.
4. Enter a name for the LDAP connection. Each LDAP connection must have a unique name.
5. In the **Server Name** field enter the name of the LDAP server that you want to connect to.
6. To make it compulsory that Websense Email Security use a user name and password to log on to the LDAP server, select **Log on to the server** and enter the user name and password to be used by Websense Email Security.
7. To specify additional information about the LDAP server, click the **Advanced** tab.
8. In the **LDAP Port number** field enter the LDAP port number.

   Default = 389

9. Select **Use Secure Connection** to use a secure connection (SSL) to connect to the LDAP server.
10. Select search base details for users and groups.

    The information for LDAP users and groups is not stored on the Websense Email Security server; it is requested from the LDAP server as necessary. Therefore specifying a Search Base makes the connection more efficient for locating specific users or groups.

    You can also choose to have either a full sub-tree search or a one-level search performed for users and groups. Full sub-tree searching should be used only by small organizations.

11. In the **Search timeout (seconds)** text box enter the amount of time that Websense Email Security will search for users and groups before timing out.

    Default = 120 seconds.

12. In the **Maximum number of search results** text box enter the maximum number of users and groups to be included.

13. Click **OK**.

Enabling Domain Substitution

You can use domain substitution only after you have enabled DHD.

To enable domain substitution:

1. Select **Enable Domain Substitution Check**.
2. Click **Domain Substitution** and click **Add**.
3. Enter the domain and click **OK**.
4. Add or edit more domains as needed and then click **OK** to return to the Server Configuration screen.

Excluding legitimate email addresses or domains

To exclude 1 or more legitimate email addresses or domains:

1. Click **Exclude**. The **Exclusion from LDAP Lookup** dialog box displays.
2. If the email address or domain is not in the list click **Add**. The **SMTP List Entry** dialog box displays.
3. Enter the email address or domain and click **OK**. The address or domain is added to the list in the **Exclusion from LDAP Lookup** dialog box.

Denial of Service (DoS) detection

A Denial of Service (DoS) attack attempts to stop a network from functioning by flooding it with useless traffic or using up network resources. DoS attacks can take many forms. A well known example is the “Ping of Death” that attempts to disrupt network traffic by repeatedly sending packets of data that exceed the standard length.

Websense Email Security can detect when servers are trying to launch a DoS attack by monitoring the number of incomplete SMTP sessions per hour. (An incomplete SMTP session occurs when a connection is made but no email is received.) When the Receive Service is restarted, the count is reset to zero.

Enabling Denial of Service detection:

1. In the Server Configuration console select

   Email Connection Management > Denial of Service Detection.
2. Select **Enable Denial of Service detection**.
3. Specify the number of incomplete SMTP sessions that Websense Email Security will accept per IP address per hour.

   Default = 30
4. Specify the action that Websense Email Security will take if a single IP address attempts more than the specified incomplete SMTP sessions per hour:
   - **Log only** – Log the DoS attack in the System Log and the Monitor.

- **Deny connections from IP for** - Deny connections for the specified number of hours.

  Default =24 hours

Excluding legitimate email addresses or domains

To exclude 1 or more legitimate IP addresses:

1. Click **Exclude**.

   The **Exclusions from Denial of Service Detection** dialog box displays.
2. If the IP address is not in the list, click **Add**. The **SMTP List Entry** dialog box displays.
3. Enter the IP address, and then click **OK**. The address or domain is added to the list in the Exclusion from LDAP Lookup dialog box.

Remote User Authentication

Use the Remote User Authentication function to configure email access for users who need to connect to your email server from outside the protected domain. For example, home workers using a dial-up connection.

If you have a large number of users you want to configure, you can create a list as a text file and import it into Websense Email Security. See *Importing a list of remote users*, page 63.

To setup Remote User Authentication:

1. In the Server Configuration console select the **Remote User Authentication** function.
2. Click **Add**. The **User Authentication Information** dialog box displays.
3. Give the remote user a user name and password. The remote user must use this name and password when logging on to Websense Email Security.
4. Click **OK**. The user name is displayed in the right panel of the Remote User Authentication screen.

Importing a list of remote users

If you have large numbers of remote users to configure, you can create a list as a text file and import it into Websense Email Security.

There are 2 stages in this process: creating the text file and importing the file.

Creating the text file:

1. Create a new .txt file with any text editor.
2. In the text file, list the remote users. Each item on the list must have the following syntax:

   `SEFAUTH;user name;password<CR><LF>`

Examples:

```
SEFAUTH;Rachel;abcd1234<CR><LF>
SEFAUTH;Barney;xyz987<CR><LF>
SEFAUTH;Homer;a1b2c3d4<CR><LF>
SEFAUTH;Marge;z9y8x7<CR><LF>
```

3. Save the file to a location that is accessible to the Websense Email Security server. Saving to the **Websense Email Security** folder saves time because the import facility looks in that folder first.

Importing the file:

1. In the Server Configuration console select

   Email Connection Management > **Remote User Authentication**.
2. Click **Import**.
3. Select the file to import and click **Open**.

If the file imports successfully, a confirmation message is displayed and the users are displayed in the right panel.

If the file does not import successfully, check that all items on the list have the correct syntax.

SPF Check

Sender Policy Framework (SPF) verifies a sender's email address, targets email spam, and fights return-path address forgery, which makes it easier to identify spoofs.

An SPF check determines if a client or mail server is authorized to send email with a given "mail from" identity.

To set up SPF checking:

1. In the Server Configuration console select the **SPF Check** function.
2. Select **Perform SPF checking against email sender**, and then select an option for the connections that the check applies to.
   - **for all connections**
   - **for all connections except when Connection Management uses True Source IP** – If you have set up mail relays to use True Source IP (see *Adding a Mail Relay*, page 45), you can use this option to remove SPF checking against senders using those mail relays.
3. Select the conditions that are needed to reject email from senders.

   Note

   Some options might block legitimate mail servers. You should exclude these legitimate servers from the SPF check.

4. To exclude legitimate servers from the SPF check, click **Exclude**. The **Exclusion from SPF check** dialog box displays.

5. If the IP address of the legitimate server is not in the list, click **Add**. The **Excluded servers list entry** dialog box displays.
6. Enter the IP address of the server and click **OK**.

Configuring the Rules Service

Websense Email Security works by checking email against the rules you specify. In this way it implements and enforces your Acceptable Use Policy (AUP).

The Rules Service controls how email is checked and processed. It is very important to configure the Rules Service with care otherwise email may not be processed against the rules you have enabled.

To configure the Rules Service you need to check and adjust the following settings:

- *Rules Service general settings*, page 65
- *Rules Service Configuration settings*, page 67
- *Queue management*, page 68

Rules Service general settings

The Rules Service general settings define the:

- Location of the folders used by the Rules Service to access, hold, and act upon email
- Use of Administrator alerts
- Where logging information is sent

To modify the Rules Service general settings open the **Server Configuration** console and select **Rules Service**. The **Rules Service** general settings display.

Rules Service folders

There are 3 folders used by the Rules Service to pick up, store, and act on email.

Warning

The path of the Rules mail pickup folder must be exactly the same as the received mail drop-off folder.

Folder	Function	Default path
Rules mail pick-up folder (**In** folder)	The Rules Service monitors this folder for incoming email.	C:\Program Files\Websense Email Security\In

Folder	Function	Default path
Work folder (**Work** folder)	Email is held in this folder while it is being checked against the rules.	C:\Program Files\Websense Email Security\Work
Processed mail drop-off folder (**Out** folder)	If an email has been checked against the rules and allowed to proceed, it is placed in the Processed mail drop-off folder. If it has been delayed or isolated it is placed in the folder specified by the rule it triggered.	C:\Program Files\Websense Email Security\Out

You can edit the paths or **Browse** to specify another location.

Enabling Administrator alerts

A robust alert system is hosted by the Dashboard. Use of that system is highly recommended. See *Using the Alerts panel*, page 111.

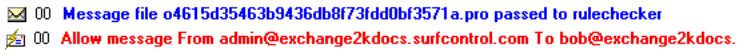
Independent of the Dashboard, the Rules service can log a message in the Windows Event log when the number of pending messages in the **\Out** folder exceeds a threshold.

Check **Enable Administrator alerts** and set a value. Default = 1000.

Logging Options

The Rules Service logging options control how the actions of the Rules Service are recorded and where they are displayed.

Select the logging options you want to enable.

Logging option	What happens when enabled
Real-time console	The actions of the Rules Service are displayed in the real-time console:  See *Service panels*, page 100.
System Log	The status of the Rules Service is displayed in the System Log in Message Administrator. For example, if you add and activate a new rule, a message is displayed, indicating that the rules configuration has been reloaded:  See *Working with logs*, page 212.

Related topics

- *Configuring the Rules Service*, page 65
- *Rules Service Configuration settings*, page 67
- *Queue management*, page 68

Rules Service Configuration settings

To change the Rules Service Configuration settings:

1. Open the Monitor and select **File > Server Configuration**. The **Server Configuration** console displays.
2. In the left panel select the function **Rules Service > Configuration**.

The **Rules Service Configuration** settings are displayed in the right panel.

Examine and edit the **Number of Rules processing threads** and **Corrupted Messages** fields.

Number of Rules processing threads

Specify the number of messages that the Rules Service can process at any one time.

Default = 4

Maximum = 16

Each thread requires approximately 16 MB of memory above the minimum system requirement of 512 MB RAM.

Warning

If there are too many Rules threads for your system to handle with its available memory, Websense Email Security will not function.

In a multiple-server configuration, this number can be set on a per-machine basis, to allow server machines with different processing speeds to handle messages efficiently.

Corrupted email

If an email has been corrupted, the Rules Service may not be able to check it against the enabled rules. You can specify how Websense Email Security behaves in the event that an email becomes corrupted.

Action	What happens
Release corrupted messages	The corrupted email is not checked by the Rules Service, and is sent directly to its recipient. A copy of the email is left in the **In** folder.
Move corrupted messages to folder	The corrupted email is moved to the folder that you specify. Enter or browse to the path of the folder.
Copy to folder and send corrupted message	Websense Email Security takes a copy of the corrupted email, saves it in the folder that you specify, and then sends the original to its recipient. Enter or browse to the path of the folder.

Queue management

If the Rules Service detects that an email has triggered a rule, the automatically managed actions that Websense Email Security can take are:

- Discard the email
- Release the email
- Isolate the email
- Delay the email

Email that is **isolated** or **delayed** is held in dedicated queue folders until it is either discarded or released and sent to its recipient. Websense Email Security is installed with predefined queues for easy management of email. You can set up additional queues to suit your needs.

To work with Queue Management settings:

1. Open the Monitor and select **File > Server Configuration**. The **Server Configuration** console displays.

2. In the left panel, click **Rules Service > Queue Management**. The queue management settings are displayed in the right pane.

Related topics

- *Adding a queue*, page 69
- *Editing a queue*, page 69
- *Deleting a queue*, page 69
- *Configuring a queue*, page 70
- *Configuring Queue Administration*, page 71
- *Automated Queue Management*, page 71
- *Using a queue for auditing*, page 72

Adding a queue

To add a queue:

1. In the Server Configuration console select

   Receive Service > Rules Service > Queue Management.
2. Click **Add**. The **Queue Configuration** dialog box displays.
3. In the **Queue Name** box enter the name of the queue you want to create, for example, Gambling.
4. In the **Queue Folder** box enter the path where you want the folder to be located.
   - To find a folder, click **Browse**.
   - To create a new folder click **New Folder** and enter the path and name of the folder in the text box.
5. Next either:
   - Click **OK** to accept the defaults
   - Configure the queue. See *Configuring a queue*, page 70.

Editing a queue

To edit a queue:

1. In the Server Configuration console select the **Queue Management** function.
2. Select the queue to be changed and click **Edit**. The **Queue Configuration** dialog box displays.
3. You cannot change the name of the queue, but you can save it to a different folder by browsing to an existing folder or creating a new folder.

You can now configure the queue. See *Configuring a queue*, page 70.

Deleting a queue

To delete a queue:

1. In the **Server Configuration** console select the **Queue Management** function.
2. Select the queue to delete and click **Delete**.
3. Confirm that you want to delete the queue.

> **Note**
> You cannot delete a queue that contains email or that is being used by a rule.

Configuring a queue

When you have entered the queue name and set up the queue folder you can configure the details. To add a queue, see *Adding a queue*, page 69.

Queue management options include:

Option	What it does
Use Queue for Auditing	You can designate the queue for the special purpose of auditing. Audit queues are used only with Personal Email Manager (PEM) and are managed through Message Administrator and Automated Queue Management. The purpose of an audit queue is to keep a copy of each email released from a PEM-monitored isolation queue at the request of the recipient. For more information, see *Using a queue for auditing*, page 72. **Note:** The "PEM Audit" queue is created automatically during installation as an audit queue for Personal Email Manager. If you are using automated queue management, the **Automated Action** menu is unavailable; the only automated action possible is **Delete**.
Queue Administration	If there are multiple email administrators in your organization you can assign administrators to queues for the management of email. Select either: • **All Users** – All administrators will be able to view, release, delete and move email held in this queue. • **Selected Users** – In the list that displays, select the check boxes of the email administrators who should have access to this queue. If there are no administrators in the list, you need to configure administrator accounts. See *Configuring administrators for remote access*, page 87.
Automated Queue Management	Automated Queue Management allows you to automatically release, delete or move isolated email at a set time. See *Automated Queue Management*, page 71.
Administrator alerts	Websense Email Security can automatically log an event in the Windows Event log when the number of messages in that queue reaches a set number. See *Enabling administrator alerts*, page 34.

Configuring Queue Administration

To configure queue administration:

1. In the Server Configuration console select the **Queue Management** function.
2. Select a queue and click **Edit**. The **Queue Configuration** dialog box displays.
3. Select **All Users** to make the queue available to all systems administrators. This means that all email administrators are able to view, release, delete and move email held in this queue.
4. Select **Selected Users** to restrict the queue to selected email administrators.

   Available email administrators are displayed in the box. Select the check boxes of the email administrators that are to have access to this queue.

   The box is blank if there are no administrator accounts. See *Adding a Remote Administrator account*, page 89.

Automated Queue Management

You can automatically delete, release or move email that has been isolated or delayed for a specified amount of time.

To add a queue, see *Adding a queue*, page 69.

To enable and configure Automated Queue Management:

1. In the **Server Configuration** console select the **Queue Management** function.
2. Select the queue and click **Edit**. The **Queue Configuration** dialog box displays.
3. Select **Enable Automated Queue Management.**
4. Select the action to be applied to the email in the queue:
   - **Release** – Release each email from its current queue folder a set time after it is placed there.
   - **Delete** – Permanently delete each email a set time after it was placed in its current queue folder.

     This is the only option if you have selected to use the queue for auditing.
   - **Move to** – Move each email to the specified queue a set time after it was placed in its current queue. Each queue is listed and when you add a new queue it will be added to the list.

     Note

     If you have selected to use the queue for auditing, this list is unavailable. The only automated action is **Delete**.
5. To specify the time for the action select **Configure**. The **Configure Automated Queue Management** dialog box displays.
6. To set the timing, select an option:
   - **Take Action after Time Delay** – The period of time that each email will be held in the queue before an action is applied to it.

Minimum = 5 minutes

- **Take Action at Specified Times**
  a. Click **Add**. The **Time of Action** dialog box displays.
  b. Enter the time for the action.
  c. Click **OK**. The time is displayed in the **Automated Queue Management** dialog box.

  To notify the email queue administrator of the action select **Notify Email Administrator of Action**.

7. To keep a record of the email that has been deleted or released by Automatic Queue Management, click **Log to the system database**. If you have selected to automatically move email to another queue, these cannot be logged and the check box is unavailable.
8. Click **OK**.

Using a queue for auditing

Audit queues are used in conjunction with Personal Email Manager (PEM) to retain a record of messages released from PEM-monitored isolation queues at the request of the recipient. This provides a method of monitoring compliance with an organization's Acceptable Use Policy (AUP).

For example, Websense Email Security may isolate a message because its contents are identified as a job recruiting newsletter and the organization has a published policy that prohibits employees from looking for work using company resources. If, through Personal Email Manager, the recipient releases the message for delivery, a copy of the email is retained in the audit queue. The organization can examine the audit queue to locate evidence of a breach of policy.

A queue can only be designated an audit queue when it is created. Use the following steps to create an audit queue:

1. Open the Server Configuration dialog. In the Rules Service section, click **Queue Management**.
2. In the Queue Management window, click **Add**.
3. In the Queue Configuration dialog, select **Use Queue for Auditing**.

> **Note**
> The "PEM Audit" queue is created automatically during installation as an audit queue for Personal Email Manager.

After creation, an audit queue is configured in Personal Email Manager on the **Configure Queue - <queue name>** page. See the section titled "Configuration page" in *Personal Email Manager Administrator's Guide*.

For PEM-monitored isolation queues, a copy of a message is retained in the audit queue when:

- A recipient releases an isolated message for delivery (the recipient must have permission to release to themselves; see *Personal Email Manager Administrator's Guide*).
- A recipient is allowed to use the Always Allowed list, and PEM is configured to keep a copy (see *Personal Email Manager Administrator's Guide*).

A copy is *not* kept in the case that a message is released after *review.* A release for review requires action from a designated review authority (a person).

When automated queue management is used with an audit queue, the **Automated Action** menu is unavailable. The only automated action possible is **Delete**. You can still move email from other queues into the audit queue.

Configuring the Send Service

The Send Service controls what happens to email after it has been allowed to proceed through the system by the Rules Service. It is important to configure the Send Service correctly, otherwise email that passes through the system will not reach its intended recipients.

To configure the Send Service you need to review and set:

- *Send Service - general settings*, page 73
- *SMTP properties*, page 74
- *Connections*, page 76
- *Routing*, page 77
- *Smart Host routing*, page 82
- *Requeuing*, page 84

Send Service - general settings

To change the Send Service properties:

1. Open the Monitor and select **File > Server Configuration**. The **Server Configuration** console displays.
2. In the left panel select **Send Service**. The **Send Service Properties** are displayed in the right panel.

Send Mail Pick-up folder

Warning

The Send Mail Pick-up folder must always be the same folder as the Rules Service Processed Mail folder.

When an email has been checked and allowed to proceed, it is placed in the Send Mail Pick-up folder (**\Out** folder), where the Send Service can pick it up for delivery. The default path is:

C:\Program files\Websense Email Security\Out

You can change the path or **Browse** to a different location.

Enabling administrator alerts

A robust alert system that includes queue size alerts, is hosted by the Dashboard. Use of that system is highly recommended. See Using the Alerts panel.

Independent of the Dashboard, you can elect to log a message in the Windows Event log when the number of queued messages in the **\Out** folder exceeds a limit.

Logging

When an email is moved to the **\Out** folder for delivery, you can log the action in 2 places.

Option	What it does
Real-time console	Details of email placed in the **\Out** folder are displayed in the Receive console of the Monitor. See *Service panels*, page 100.
System log	System events related to the Send Service are displayed in the System log in Message Administrator. See *Working with logs*, page 212.

SMTP properties

The configurable SMTP properties are:

- *SMTP EHLO/HELO command*, page 75
- *Email transmission optimizations*, page 75

SMTP EHLO/HELO command

The SMTP EHLO/HELO command is the SMTP statement that will be used to make an SMTP connection with the receiving mail server to send the email in the **\Out** folder. There are 2 ways that Websense Email Security can connect.

Setting	What happens
Use the Windows computer name as the Domain name	When Websense Email Security initiates the outbound connection, the EHLO/HELO statement uses the host name of the machine where Websense Email Security is installed as a domain name, for example: `HELO devserver`
Specify the Domain name	When Websense Email Security initiates the outbound connection, the EHLO/HELO statement contains the domain name you specify, for example: `HELO mycompany.com`

Related topics

- *SMTP properties*, page 35
- *Email transmission optimizations*, page 75

Email transmission optimizations

Websense Email Security supports 2 methods of optimizing email Receive and Send transmission: CHUNKING and PIPELINING.

Warning

These features are disabled by default because some external servers do not support pipelining or chunking.

Use caution when enabling these options.

For more information, go to the Websense knowledge base portal at Websense.com and search for “pipelining chunking”.

Setting	What happens
Enable CHUNKING	The size of each SMTP data chunk is sent with the data. This means that the SMTP host does not have to scan continuously for the end of the data. This improves the speed of transmissions.
Enable PIPELINING	Provides the ability to send a stream of commands without having to wait for a response after each command. This improves the speed of transmissions.

Related topics

- *SMTP properties*, page 35
- *SMTP EHLO/HELO command*, page 75

Connections

The Connections function controls the type and number of connections that Websense Email Security can make when it is sending email. The configurable connection settings are:

- Connection properties
- SMTP options.

Connections properties

You can change the following settings:

Option	Description	Default	Maximum
Maximum active outbound connections	The maximum number of outbound connections that Websense Email Security can make at any one time.	200	1000
Maximum connections per IP address	The maximum number of outbound connections that Websense Email Security can make to any single IP address. **Note:** This number must be less than, or equal to, the maximum active outbound connections.	10	1000
Idle connection timeout	The number of seconds after which Websense Email Security will drop an attempted connection.	300	3600

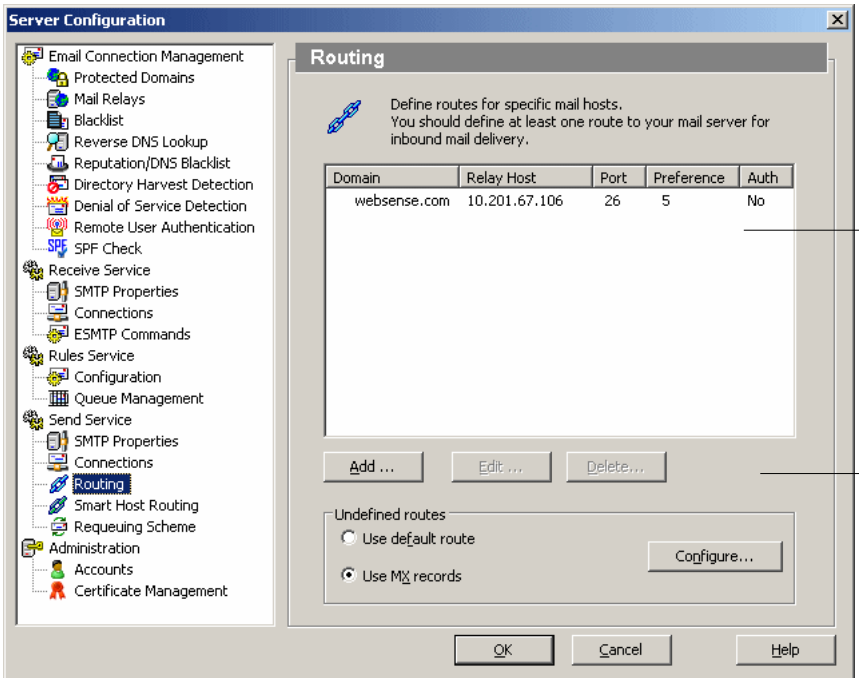
SMTP options

To limit the amount of email sent through a single connection:

1. In the SMTP options area select **Limit maximum messages per connection**.
2. Enter or scroll to the maximum number of messages for a single connection.

Routing

Use Routing to define routing tables for Websense Email Security.



The routing table defines the location of your email servers so that Websense Email Security can determine where to send email within the protected domain.

To define a static route, see *Static Routes*, page 78.

To define a relay host, see *Configuring a default route*, page 79.

To use DNS to route mail to undefined domains, see *Configuring MX lookups*, page 81.

Related topics

- *Configuring a default route*, page 79
- *Routing to sub-domains*, page 77

Routing to sub-domains

Unless you add the specific details of a sub-domain, email sent to sub-domains is sent using the route defined for the parent domain. You can either:

- Add the details of sub-domains directly to the routing table. See *Static Routes*, page 78.
- Add a domain and then select the option **Treat routing for sub domains as a separate domain** in the **Domain Route Properties** dialog box. This means that all sub-domains of the specified domain are treated as undefined routes. See *Configuring a default route*, page 79 and *Configuring MX lookups*, page 81.

Static Routes

By default, the protected domain specified during installation is listed in the Static Routes list.

If your organization has more than 1 protected domain, you need to add the other domains that were not specified during installation. You can also add details of sub-domains or an external mail server, for example, if your organization generates a lot of email traffic with a particular company.

To add a static route:

1. In the Server Configuration console select **Send Service > Routing**.
2. Click **Add**. The **Domain Route properties** dialog box displays.
3. In the **Domain Name for Static Route** text box, enter the domain name.
4. In the **Route Host for this Domain** text box, enter the IP address of a server that you want to handle email for this domain.
5. In the **IP port to use for this SMTP host** text box, enter the port number of the server you want to handle email for this domain.

   Default = 25
6. Set the **Preference** number for the route.

   Default = 5

   If multiple routing entries are defined for a single route, Websense Email Security attempts to send email to routes in order of preference, from the lowest (1) to the highest.

   If 2 or more routes have the same preference, Websense Email Security selects a random order for the routing.
7. Select **Treat routing for sub domains as a separate domain**, if needed. See *Routing to sub-domains*, page 77.
8. Select **Server Requires Authentication** if Websense Email Security needs to supply authentication details to connect to the server. Enter a valid user name and password.
9. Select **Send message encrypted** to force the mail server to accept only encrypted connections using TLS (STARTTLS) or SSL (SMTPS).

   Default = Cleared

Static route options:

Option	Description
Always use STARTTLS	Messages are sent via an encrypted connection using TLS. If the email server does not support TLS, or the STARTTLS operation fails, the Send Service: • Sends a warning message, which is also logged in the system log. • Temporarily fails the email and requeues it.
Use STARTTLS if available, otherwise send unencrypted	Messages are sent encrypted using TLS. However, if the mail server does not support TLS, the email is sent unencrypted.
Use SMTPS on port	Default (recommended) port = 465 Messages are sent encrypted using SSL. If the mail server does not support SSL, or the SMTPS operation fails, the Send Service: • Sends a warning message, which is also logged in the system log. • Temporarily fails the email and requeues it.

When you have added static routes, you need to specify how Websense Email Security will route email addressed to destinations outside the domains specified on the Static Routes list. You can:

- Use a default route that you specify.

  The Send Service passes any email addressed to domains not on the Static Routes list to the server you specify as the default route. This server then handles the email and performs the MX lookups to send the email to its destination.

  The default route is initially the route you specified during installation, but you can change its details or add further servers. See *Configuring a default route*.

- Use MX records

  Websense Email Security attempts to route the email by performing the MX lookups itself. See *Configuring MX lookups*, page 81.

Configuring a default route

The Send service passes email addressed to domains not on the Static Routes list to the server you specify as the default route. This server handles the email and performs the MX lookups to send the email to its destination.

The default route is initially the route you specified during installation, but you can change its details or add other servers.

By default, the default route is the server you specified during installation.

To add or change the default route:

1. In the **Server Configuration** console select **Send Service** > **Routing**.
2. In the **Undefined routes** area select **Use default route**.

3. Click **Configure**. The **Default Routes Configuration** dialog box displays.
4. You can either:
   - Select the default server and click **Edit**.
   - Click **Add** to add another server.

   The **Domain Route properties** dialog box displays.
5. The name in the **Domain Name for Static Route** field is always **Default**.
6. In the **Route Host for this Domain** field, enter the IP address of the server you want to use as the default route.
7. In the **IP Port to use for this SMTP Host** field, enter the IP port that Websense Email Security will use to communicate with the server.

   Default = 25
8. Set the **Preference** number for the route.

   Default = 5

   If multiple routing entries are defined for a single route, Websense Email Security attempts to send email to routes in order of preference, from the lowest (1) to the highest.

   If 2 or more routes have the same preference, Websense Email Security selects a random order for the routing.
9. If the **Server Requires Authentication**, enter a valid user name and password. Confirm the password.
10. Select **Send message encrypted** to force the email server to accept only encrypted mail using TLS (STARTTLS) or SSL (SMTPS).

    Default = Cleared

Option	Description
Always use STARTTLS	Messages are sent via an encrypted connection using TLS. If the email server does not support TLS, or the STARTTLS operation fails, the Send Service: • Sends a warning message, which is also logged in the system log. • Temporarily fails the email and requeues it.
Use STARTTLS if available, otherwise send unencrypted	Messages are sent encrypted using TLS. However, if the email server does not support TLS, the messages are sent unencrypted.
Use SMTPS on port	Default (recommended) port = 465 Messages are sent encrypted using SSL. If the email server does not support SSL, or the SMTPS operation fails, the Send Service: • Sends a warning message, which is also logged in the system log. • Temporarily fails the email and requeues it.

11. Click **OK**. The dialog box closes and the server details are listed in the **Default Routes Configuration** dialog box.

12. Click **OK** to return to the Server Configuration console.

Configuring MX lookups

If you do not use a Relay Host to route outbound email you need to configure Websense Email Security to perform a DNS query to determine the correct mail server for the recipient email domain.

1. In the Server Configuration console select **Send Service > Routing**.
2. In the **Undefined routes** area select **Use MX Lookups** and click **Configure**. The **MX Lookup Properties** dialog box displays.
3. **Direct Connections:**

   If a domain exists, but Websense Email Security cannot find an MX record for it, it can try to connect to the domain's A record using port 25.

   Specify the action you want Websense Email Security to take if an MX Lookup fails:

   - Always try direct connections
   - Never try direct connections

   The timeout value for direct connections is 60 seconds, so attempting direct connections can delay the delivery of mail.
4. **Caching Options:**
   a. Select **Cache MX records** if you want MX records to be cached. Specify how long you want MX records to be cached. Maximum = 24 hours
   b. Select **Cache non-existent domains** to cache non-existent MX records. Specify how long you want the non-existent records to be cached. Maximum = 24 hours

      If a non-existent MX record is cached, Websense Email Security will not attempt further MX lookups for that domain.
5. **Send mail encrypted**:

   You can elect to send email encrypted using TLS.
   a. To add a domain and set the TLS policy, click **Add**. The **Domain - TLS Properties** dialog box displays.

      Enter the domain name.

      Optionally enter a description.

      Select a TLS policy.

      If you select **TLS is required for this domain** and the domain does not support TLS, messages sent to that domain will fail to be delivered.
   b. To edit an existing entry, select the entry and click **Edit**. The **Domain - TLS Properties** dialog box displays.

      Make changes as required.

      If you select **TLS is required for this domain** and the domain does not support TLS, messages sent to that domain will fail to be delivered.
   c. To delete an entry, select the entry, click **Delete**, and confirm the action.

d. To use TLS, if available, for all other domains, select **For all other domains, use TLS if available**. Default = cleared

6. Click **OK** to save your changes and return to the Server Configuration console.

Smart Host routing

You can route email to a specific mail server or Message Transfer Application (MTA) according to its content, for example:

- If your organization uses an encryption server, Websense Email Security can redirect email that meets the criteria you specify for encryption. The encryption server encrypts the email and sends it to its destination.
- If your organization has an archiving policy, Websense Email Security can send a copy of each email that meets your archiving criteria to the archiving server, while processing the original email as usual.

Enabling Smart Host routing

Before you configure Smart Host Routing, make sure that the Smart Host server can accept email from the Websense Email Security Send Service. Consult your Smart Host documentation for more information on how to do this.

When you have enabled the Smart Host to accept mail, you need to:

1. Configure Smart Host Routing in the Server Configuration console.
2. Set up a rule in the Rules Administrator that specifies the email you want to be routed to the Smart Host. See *Routing object*, page 186.

Configuring Smart Host routing

Note

Smart Host routing supports fail-over. If you configure more than one relay host, the Send Service will try to send email to the first relay host on the list. If it cannot send to that relay host, it will try each one in order. If the Send Service cannot send the email to any of the Relay Hosts, the email is requeued.

To configure Smart Host Routing:

1. In the Server Configuration console select **Send Service > Smart Host Routing**.
2. Click **Add**. The **Smart Host Properties** dialog box displays.
3. In the **Smart Host Name** text box, enter the name of the Smart Host server to which you want email redirected.
4. Click **Add**. The **Relay Host properties** dialog box displays.
5. **Relay Host** - Enter the DNS server name or IP address of the Smart Host to which email is redirected, for example, the encryption server.

6. **IP port for this SMTP host** - Enter the IP port number of the server that will handle email for this domain.

   Default = 25

7. **Preference** - Set the preference number for the route.

   Default = 5

   If multiple routing entries are defined for a single route, Websense Email Security attempts to send email to routes in order of preference, from the lowest (1) to the highest.

   If 2 or more routes have the same preference, Websense Email Security selects a random order for the routing.

8. **Server Requires Authentication** - If Websense Email Security needs to be authenticated by the Smart Host, select the **Server Requires Authentication** box, and enter the user name and password of an account that will be accepted by the Smart Host.

9. **Send message encrypted** - You have the option to force the mail server to accept only encrypted email using TLS (STARTTLS) or SSL (SMTPS). Select **Send message encrypted**.

   Default = Cleared

   See the table below for a description of the options.

10. Click **OK**. The details of your Smart Host server are displayed in the **Smart Host Properties** dialog box.

11. Click **OK**.

You have configured a Smart Host. To route email to this server when one triggers a rule, set up a rule containing the Routing object. See *Routing object*, page 186.

Options for encrypted email:

Option	Description
Always use STARTTLS	Messages are sent encrypted using TLS. If the mail server does not support TLS, or the STARTTLS operation fails, the Send Service: • Sends a warning message, which is also logged in the system log. • Temporarily fails the email and requeues it.
Use STARTTLS if available, otherwise send unencrypted	Messages are sent encrypted using TLS. However, if the mail server does not support TLS, the messages are sent unencrypted.
Use SMTPS on port	Default (recommended) port = 465 Messages are sent encrypted using SSL. If the mail server does not support SSL, or the SMTPS operation fails, the Send Service: • Sends a warning message, which is also logged in the system log. • Temporarily fails the email and requeues it.

Deleting a Smart Host

> **Note**
> You cannot delete a Smart Host that is being used in a rule.

To delete a Smart Host:

1. Select the Smart Host you want to delete and click **Delete**.
2. Confirm the action.

Requeuing

If Websense Email Security cannot send an email, for example because it cannot connect to a remote mail host, it stores the email in a queue and tries to send it again at set intervals. You can specify how often these attempts to resend email take place. You can configure:

- How many times Websense Email Security tries to send the email.
- The length of time between each attempt.
- Whether to notify the sender after a specified number of failed retries.

You can decrease the number of attempts and increase the time between each attempt over 4 stages. The default intervals are:

Stage	Retry attempts	Retry intervals	What happens
1	12	15 min	Send once every 15 minutes for 12 attempts.
2	21	60 min	Send once every 60 minutes for 21 attempts.
3	8	360 min	Send once every 360 minutes for 8 attempts.
4	0	1440 min	Send once every 1440 minutes for 0 attempts.

You can change any of the retry attempts and retry intervals. However it is recommended that you leave the default settings unchanged.

You can also specify when an email notification of the delay or failure is sent to the sender.

To configure the requeuing options:

1. In the **Server Configuration** console select **Send Service > Requeuing Scheme**.
2. Enter new values to specify the number of attempts and the number of minutes between each attempt.
3. To send a notification to the sender after a specified number of retries, check **Notify Sender After** and specify the number of retries.
4. To delete a message that could not be delivered after all retry attempts, check **Delete dead messages after all retry attempts**.

The requeuing intervals are added together to make the total retry time. If Websense Email Security cannot send the email after the total retry time has elapsed, the email is designated a dead message.

If you do not discard dead messages automatically, they remain in the **\Out** folder indefinitely until they are deleted manually. While dead messages are held in the **\Out** folder, you can attempt to resend them using *QueueView*, page 104.

Related topics

- *Dead Messages*, page 85
- *Discard Message object*, page 195

Dead Messages

Dead messages have the file extension **.msg.d** and are stored in the **\Out** folder. When you configure the requeuing schedule, you can choose to automatically delete dead messages as soon as the total retry time is up.

To delete dead messages automatically:

1. In the Server Configuration console select **Send Service > Requeuing Scheme**.
2. Select **Delete dead messages**.
3. When the total retry time expires, the email is deleted.

Note

Deleted email cannot be retrieved.

Warning

If dead messages are allowed to build up in the **\Out** folder, performance of the Send Service may be diminished and delay the delivery of email.

If you do not discard dead messages automatically, they remain in the **\Out** folder until you delete them manually. While they are held in the **\Out** folder you can attempt to resend them using QueueView. See *The QueueView Window*, page 105.

Configuring the Administration Service

The Administration Service controls general system settings and has these functions:

- **Configuration** – to configure remote administration access to Websense Email Security.
- **Certificate Management** – to manage the certificate used for the Send and Receive services TLS and SMTPS security features.

Related topics

Administration settings - general, page 86

Setting the email address of the System Administrator, page 86

Printing the system configuration, page 87

Configuring administrators for remote access, page 87

Remote administration permissions, page 88

Adding a Remote Administrator account, page 89

Editing a Remote Administrator account, page 90

Deleting a Remote Administrator account, page 90

Certificate Management, page 91

Administration settings - general

The Administration function contains general settings for the Administration services.

On the Administration screen you can:

- Set the email address of the Websense Email Security administrator. See *Setting the email address of the System Administrator*, page 86.
- Print the system configuration to a text file. See *Printing the system configuration*, page 87.
- Enable or disable SystemSynch. SystemSynch reports systems information to the Websense Email Security download server. See *Enabling and disabling SystemSynch*, page 87.

Related topics

- *Configuring the Administration Service*, page 85
- *Configuring administrators for remote access*, page 87
- *Remote administration permissions*, page 88
- *Adding a Remote Administrator account*, page 89
- *Editing a Remote Administrator account*, page 90
- *Deleting a Remote Administrator account*, page 90
- *Certificate Management*, page 91

Setting the email address of the System Administrator

When you set up *Protected Domains*, you are asked to specify the email address of the system administrator for each domain. If Websense Email Security needs to send a

notification (for example an NDR), it examines each recipient of the email and checks each domain against the Protected Domains list. When it finds a recipient in a protected domain, Websense Email Security sends the notification from the administrator of that domain. If none of the recipients are in any of the protected domains, Websense Email Security sends the notification from the email address specified in the **Administration Settings**.

To change the System Administrator email address:

1. Open the Monitor.
2. Select **File > Server Configuration**. The **Server Configuration** console displays.
3. Select the **Administration** function.
4. In the **Email Administrator** field, enter the address that you want Websense Email Security to send notifications to if it cannot find a domain administrator.

You cannot enter more than 1 email address. However, if you create a group in Exchange that contains all the Websense Email Security administrators, you can enter the group email address, for example, WES_administrators@mycompany.com.

Printing the system configuration

To print the Websense Email Security system configuration:

1. Open the Monitor and select **File > Server Configuration**. The **Server Configuration Console** displays.
2. Click the **Administration Settings** function and click **Print Configuration**. A text file displays that shows all of the Server Configuration settings.

   By default, the name of the file is STEFCFG_*date_time* (for example STEFCFG_27_Jun_2007). You can save the file as any name in any location.

Enabling and disabling SystemSynch

When SystemSynch is enabled, Websense Email Security sends to Websense, Inc., general information about your installation, such as the Websense software version, operating system version, the optional Websense components installed, and related information. This information gives Websense, Inc., a current profile of the installation and leads to better technical support.

SystemSynch never sends information that would identify specific users.

Configuring administrators for remote access

Use the Accounts function to configure access to the Dashboard and remote administration of Websense Email Security. There are 2 methods of remote access:

- *Web Administrator*, page 241

The Web Administrator is a Web-based application that gives remote access to selected Websense Email Security functions from any computer through a Web browser.

- *Administration Client*, page 241

  You can install the Websense Email Security Administration Client on a remote computer and use it to access the Websense Email Security user interface. For details of how to install the client, see the *Websense Email Security Installation Guide*.

Related topics

- *Configuring the Administration Service*, page 85
- *Remote administration permissions*, page 88
- *Adding a Remote Administrator account*, page 89
- *Editing a Remote Administrator account*, page 90
- *Deleting a Remote Administrator account*, page 90

Remote administration permissions

These are the configurable permissions for remote administrators:

Permission setting	Access	Access method	
		Web Admin	Email Admin Client
Message Administration See *Message Administrator*, page 197.	View and work with isolated email using Message Administrator functions. You can select to enable the administrator to use the Message Search function, queues and logs; have the ability to search for a message but not view its contents; or have access only to either the queues or the logs.	Yes, except Search function	Yes
Rules Administration See *The Rules Administrator*, page 119.	Create and manage rules to enforce your organization's AUP using Rules Administrator functions.	No	Yes
System Administration	The administrator can: • View the progress of email through Websense Email Security in real-time. See *The Monitor*, page 97. • Configure Websense Email Security using the Server Configuration console. See *Setting Up Websense Email Security*, page 29.	No	Yes
Dictionary Management See *Dictionary Management*, page 215.	Manage Dictionaries and their content.	Yes	Yes

Permission setting	Access	Access method	
User Management	Set administrative access to Websense Email Security.	No	Yes
Dashboard Access	• View Dashboard contents after entering user name and password • Select the trend graphs, graph time ranges, and the Websense Email Security servers to view	No	Yes
Dashboard Administration	In addition to Dashboard Access permissions functions, view and edit Alerts and Threat Group configurations and acknowledge and dismiss alerts	No	Yes

Related topics

- *Configuring the Administration Service*, page 85
- *Configuring administrators for remote access*, page 87
- *Adding a Remote Administrator account*, page 89
- *Editing a Remote Administrator account*, page 90
- *Deleting a Remote Administrator account*, page 90

Adding a Remote Administrator account

To use Remote Administration you need to add administrator accounts and set their permissions. If there are no administrator accounts, Remote Administration is unavailable.

To add a Remote Administrator account:

1. In the **Server Configuration** console select the **Accounts** function.
2. Click **Add**. The **Administrator Account** dialog box displays.
3. Enter a user name, password, and email address for the administrator. The password must be at least 6 characters.
4. Select the permissions for the administrator. See *Remote administration permissions*, page 88.
5. The Queues list displays the queues that are available to the administrator. Use Queue Management to change these settings. See *Queue management*, page 68.
6. Click **OK** to confirm your changes and close the dialog box.

Related topics

- *Configuring the Administration Service*, page 85
- *Configuring administrators for remote access*, page 87
- *Remote administration permissions*, page 88
- *Editing a Remote Administrator account*, page 90
- *Deleting a Remote Administrator account*, page 90

Editing a Remote Administrator account

To edit a Remote Administrator account:

1. In the **Server Configuration** console select the **Accounts** function.
2. Select an administrator from the list and click **Edit**. The **Administrator Account** dialog box displays.
3. Change the user details and permissions as required.
4. Click **OK** to accept the changes.

Related topics

- *Configuring the Administration Service*, page 85
- *Configuring administrators for remote access*, page 87
- *Remote administration permissions*, page 88
- *Adding a Remote Administrator account*, page 89
- *Deleting a Remote Administrator account*, page 90

Deleting a Remote Administrator account

To delete a Remote Administrator account:

1. In the **Server Configuration** console select the **Accounts** function.
2. Select an administrator from the list and click **Delete**.
3. In the confirmation pop-up, confirm or cancel the deletion.

Related topics

- *Configuring the Administration Service*, page 85
- *Configuring administrators for remote access*, page 87
- *Remote administration permissions*, page 88
- *Adding a Remote Administrator account*, page 89
- *Editing a Remote Administrator account*, page 90

Certificate Management

You need to use a certificate for the TLS and SMTPS security features in the Send and Receive services. Websense Email Security supports 2 types of certificates:

- **Self-signed** – Self-signed certificates are useful to secure internal email traffic between mail servers because verification and authentication is not an issue; all servers are owned by the company, and therefore trusted.
- **CA** (Certification Authority) signed – You can buy a certificate from a CA, such as Thawte or Verisign. To obtain a certificate, you need to submit a CSR (certificate signing request) to the CA. These CAs only issue a certificate if they are satisfied that you own the domain that the certificate is to be issued for.

> **Note**
> Prior to managing Websense Email Security certificates, you must log in with the same user account that was specified during installation configuration. See the *Websense Email Security Installation Guide* for details. If you are logged in as a different user, TLS is not enabled and you will not be able to use your certificate, whether it is self-signed or CA signed.

To see the current certificate information, in the Administration function, click on Certificate Management. If a certificate is installed, or a certificate is installed with a pending CSR, or there is a pending CSR and no certificate installed, the relevant details are displayed.

Click the **Certificate Manager** button to open the **Certificate Wizard**. The options available in the Certificate Wizard depend on the status of your certification. The options are:

- Create a CSR.
- Create a self-signed certificate and install it.
- Assign an existing certificate, if you have one saved.
- Process a pending CSR and install the certificate.
- Delete a pending CSR.
- Remove the current certificate.

Related topics

- *Certificate Management*, page 91
- *Creating a self-signed certificate or CSR*, page 92
- *Assigning an existing certificate*, page 93
- *Processing a pending CSR*, page 94
- *Deleting a pending CSR*, page 94
- *Removing a current certificate*, page 94

Using the Certificate Wizard

In the **Certificate Management** console, click **Certificate Manager** to open the Certificate Wizard.

The options available depend on the status of your certificate. Use the Certificate Wizard to:

- Create a CSR.
- Create a self-signed certificate and install it.
- Assign an existing certificate, if you have one saved.
- Process a pending CSR and install the certificate.
- Delete a pending CSR.
- Remove the current certificate.

Warning

If you do not have a certificate installed, your server will not be able to send or receive email securely.

Related topics

- *Certificate Management*, page 91
- *Creating a self-signed certificate or CSR*, page 92
- *Assigning an existing certificate*, page 93
- *Processing a pending CSR*, page 94
- *Deleting a pending CSR*, page 94
- *Removing a current certificate*, page 94

Creating a self-signed certificate or CSR

To create a self-signed certificate or CSR, you need to enter the following information in the Certificate Wizard:

- A common name for the server.
  - If your server is on the Internet, use a valid DNS name.
  - If your server is on an Intranet, you might want to use the computer's NetBIOS name.
- An easily-remembered, "friendly" name for the certificate.
- The number of bits to be used to generate the certificate. The certificate is more secure if you select a higher number.

  Default = 1024

Note

A higher strength security key might decrease performance.

- The name of your organization and your organizational unit (division or department).
- Your geographical information.

CSR only

If you are creating a CSR, you also need to enter a file name (format *.txt) for the request file. Either accept the default file name, or enter, or browse to the location of an existing file.

When you have saved the file, send it (for example, by email) to your CA.

Related topics

- *Certificate Management*, page 91
- *Using the Certificate Wizard*, page 92
- *Assigning an existing certificate*, page 93
- *Processing a pending CSR*, page 94
- *Deleting a pending CSR*, page 94
- *Removing a current certificate*, page 94

Assigning an existing certificate

If you have an existing certificate, you can select the file from a list of available certificates in the Certificate Wizard.

Related topics

- *Certificate Management*, page 91
- *Using the Certificate Wizard*, page 92
- *Creating a self-signed certificate or CSR*, page 92
- *Processing a pending CSR*, page 94
- *Deleting a pending CSR*, page 94
- *Removing a current certificate*, page 94

Processing a pending CSR

If you select to process a pending CSR using the Certificate Wizard, enter or browse to the location of the **.cer** file that you received from the CA.

Related topics

- *Certificate Management*, page 91
- *Using the Certificate Wizard*, page 92
- *Creating a self-signed certificate or CSR*, page 92
- *Assigning an existing certificate*, page 93
- *Deleting a pending CSR*, page 94
- *Removing a current certificate*, page 94

Deleting a pending CSR

If you select to delete a pending CSR using the Certificate Wizard, any data from the pending CSR is removed, and you will not be able to process any future responses.

Note

You might want to notify your CA that your CSR has been deleted.

Related topics

- *Certificate Management*, page 91
- *Using the Certificate Wizard*, page 92
- *Creating a self-signed certificate or CSR*, page 92
- *Assigning an existing certificate*, page 93
- *Processing a pending CSR*, page 94
- *Removing a current certificate*, page 94

Removing a current certificate

If you select to remove a current certificate with the Certificate Wizard, the current certificate is removed from the server.

Warning

A certificate must be installed for the Websense Email Security server to use secure methods to receive or send email.

Related topics

- *Certificate Management*, page 91
- *Using the Certificate Wizard*, page 92
- *Creating a self-signed certificate or CSR*, page 92
- *Assigning an existing certificate*, page 93
- *Processing a pending CSR*, page 94
- *Deleting a pending CSR*, page 94

Configuration complete

When you are done making changes to the server configuration, click **OK** to confirm your changes.

Websense Email Security then stops and restarts any services that have changed in configuration.

Backing up your server configuration

You can back up the configuration settings so that you can replicate them on other servers or restore them if for any reason Websense Email Security has to be reinstalled. See *Database Tools* for more information.

4 The Monitor

Websense Email Security provides 2 tools for monitoring system activity:

- Monitor
- Dashboard

Monitor:

The Monitor shows the progress of email in real-time as it travels through Websense Email Security. The status of an email can be observed as it is processed by the Receive, Rules, and Send services.

The Monitor also provides access to other system components, including the Server Configuration console, Message Administrator, Rules Administrator, QueueView, and Scheduler.

You can start and stop the Websense Email Security services from the Monitor, as well as change the proxy server user name and password that you entered in the Configuration Wizard at product installation.

See *Monitor*, page 98.

Dashboard:

The Dashboard provides an immediate visual picture of system health and activity. What is displayed is configurable. By default the Dashboard displays:

- Cumulative filtering statistics from the date of initial deployment
- The status of ThreatSeeker technologies, such as the Reputation service, Anti-Spam Agent, and others
- Graphs of inbound connection activity, inbound filtering, and outbound filtering
- System alerts
- The number of messages in each isolation queue
- Additional information

See *Dashboard*, page 109.

Monitor

The Monitor:

- Shows the status of messages in real-time as they pass through Websense Email Security
- Provides access to other system components, including the Server Configuration console, Message Administrator, Rules Administrator, QueueView, and Scheduler
- Allows you to start and stop the Websense Email Security services
- Lets you change the proxy user name and password established in the Configuration Wizard at installation. Select the Monitor **Tools > Options** to edit the user name and password.

Opening the Monitor

To open the Monitor, select

Start > Programs (or **All Programs) > Websense Email Security > Monitor**

Parts of the Monitor

The parts of the monitor include:

The Monitor toolbar, page 99

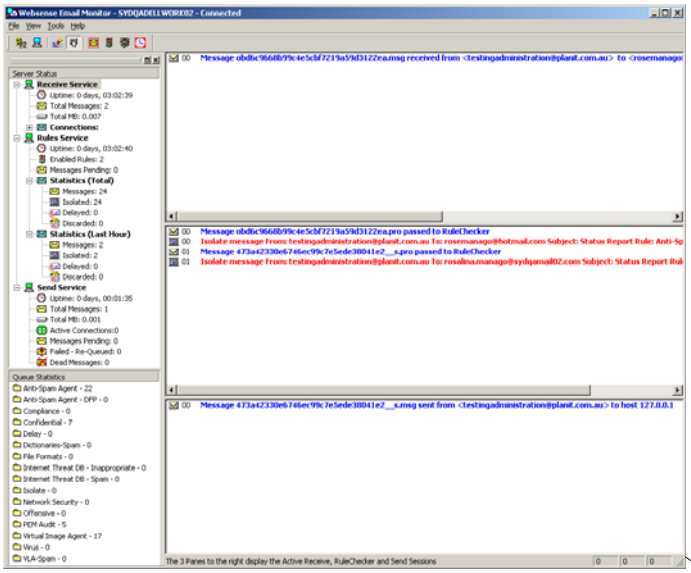
Service panels, page 100

Server Status panels, page 102

Queue Statistics pane, page 104

Status bar, page 104

The Monitor window is divided into panels, each showing information about a different part of the filtering process.



You can drag the Server Status and Queue Statistics panels anywhere on the desktop.

To hide or show the Server Status and Queue Statistics panels, click  .

The Monitor toolbar


Opens the Service Control dialog


Opens the Server Configuration console


Clears the Service panes of information


Displays or hides the System Bar


Opens the Message Administrator


Opens the Rules Administrator


Opens QueueView


Opens the Scheduler

Service panels

The Monitor includes 3 service panels that show the progress of email through Websense Email Security.

Panel	Information displayed
Receive panel	Shows Receive Service activity. When a mail server or firewall requests a connection with Websense Email Security, a log entry is displayed in this panel.
Rules panel	Shows Rules Service activity. When Websense Email Security checks an email against enabled rules, a log entry is displayed in this panel. When an email triggers an action (Isolate, Delay, Delete or Allow), the log entry text is red. A log entry is also displayed in this panel when you update the Anti-Spam Agent.
Send panel	Shows Send Service activity. When Websense Email Security delivers an email—including those released from isolate or delay queues—a log entry is displayed in this panel.

Related topics

- *Clearing the service panels*, page 100
- *Copying service panel information to the clipboard*, page 101
- *Changing the information displayed in the service panels*, page 101

Stopping and starting services

To start, stop, or pause Websense Email Security services:

From the Service Control icon:

1. Click the Service Control icon  on the Monitor toolbar. The Service Control dialog box is displayed.
2. Select the service you want and click Start, Stop or Pause.

From the system tray:

- Right-click the Monitor  icon in the system tray to display the shortcut menu. Select the desired service control action.

Clearing the service panels

To clear all 3 service panels together, click the  on the Monitor toolbar.

To clear 1 service panel:

1. Right-click the service panel. A shortcut menu is displayed.

2. Select **Clear <Receive/Rules/Send> Console**. All information is cleared from the selected panel.

As soon as there is a new event, for example, the service is restarted or the service handles an email, log entries are again displayed in the service panel.

Copying service panel information to the clipboard

You can copy service panel information to the clipboard to paste into another application, for example Notepad.

1. Right-click a service panel. A shortcut menu is displayed.
2. Select **Copy contents to Clipboard**.
3. Paste the information into another application.

Changing the information displayed in the service panels

You can specify how much detail you want displayed in each service panel by changing the logging level. There are 4 logging levels.

Note

It is recommended that you keep the logging level set to 0 or 1. You may need to set the level higher if you are working with Websense Technical Support to investigate a problem.

- Level 0: Basic email processing status is logged. For example:
  - When the receive or send services accept or send an email (blue text).
  - If the email has triggered a rule.
- Level 1: More detailed information about service activity is logged. For example:
  - SMTP conversations between the Receive and Send services and the connecting client.
  - The status of rule the checking process.
- Levels 2 and 3: Very detailed information used for diagnostic purposes is logged. If you are working with Websense Technical Support, you may be asked to increase the logging level to 2 or 3.

Changing the Logging Level

To change the logging level:

1. Right-click the service panel to change. A shortcut menu is displayed.
2. Select **Console Logging Level** and select the logging level.

   0 = least detail

   3 = most detail.

3. If you do not want information messages to be displayed, for example notification of configuration reloads, select **Hide Info Messages**.

Server Status panels

The Server Status panels show information about active services and the connections they are making.

> **Note**
> To stop, start, and pause services from the Server Status panel, right-click the service and select an action.

Information displayed in the Server Status panels

The Receive Service panel:

Section		Information displayed
Uptime		Time since the Receive Service was last started.
Total messages		Number of email messages handled by the Receive Service during Uptime.
Total MB		Amount of data in MB handled by the Receive Service during Uptime.
Connections	Total	Total number of connections accepted during Uptime.
	Active	Number of connections currently active.
	Denied	Number of connections denied during Uptime.

The Rules Service panel:

Section	Information displayed
Uptime	Time since the Rules Service was last started.
Enabled Rules	Number of rules currently enabled.
Messages Pending	Number of email messages in the **In** folder awaiting checking against enabled rules.

Section		Information displayed
Statistics (Total)	Messages	Number of email messages checked by the Rules Service during Uptime.
	Isolated	Number of email messages moved to an Isolate folder during Uptime.
	Delayed	Number of email messages moved to the Delay folder during Uptime.
	Discarded	Number of email messages discarded during Uptime.
Statistics (Last Hour)	Messages	Number of email messages checked by the Rules Service in the last hour.
	Isolated	Number of email messages moved to an Isolate folder in the last hour.
	Delayed	Number of email messages moved to the Delay folder in the last hour.
	Discarded	Number of email messages discarded in the last hour.

The Send Service panel:

Section	Information displayed
Uptime	Time since the Send Service was last started.
Total Messages	Total number of email messages delivered by the Send Service during Uptime.
Total MB	Total amount of data in MB handled by the Send Service during Uptime.
Active Connections	Number of connections currently being made by the Send Service.
Messages Pending	Number of email messages in the Out folder awaiting delivery.
Failed – Requeued	Number of email messages that have been requeued because of a temporary failure to connect to the intended mail server.
Dead Messages	Number of email messages that could not be delivered and have been designated dead messages.

Clearing the statistics

When you start or restart the Rules Service, the Statistics (Total) and the Statistics (Last hour) are reset to 0. To reset these statistics while the service is running, right-click **Rules Service** and select **Clear Statistics**.

Queue Statistics pane

The Queue Statistics pane shows all of the configured queues and the amount of email in each queue.

Double-click on a queue to view the contents in the Message Administrator.

Status bar

From left to right, the Status bar shows the status of the 3 core services.

Field position	Service	What it shows
Left	Receive Service	The number of current Receive Service connections.
Middle	Rules Service	The number of active Rules processing threads. This number is equal to the number of email messages actively being processed by the Rules Service.
Right	Send Service	The number of Send Service connections.

- If a service is stopped, an "**X**" is displayed in its status field.
- If a service is running but a connection cannot be made, a "**?**" is displayed.
- If a service is paused, a "**P**" is displayed in its status field.

Related topics

- *Configuring the Receive Service*, page 33
- *Configuring the Rules Service*, page 65
- *Configuring the Send Service*, page 73

QueueView

If an email cannot be delivered immediately it is held in a queue while Websense Email Security attempts to deliver it. You can view the status of queued email in the QueueView window.

Opening QueueView

Open QueueView from the Start Menu or within the Monitor.

From the Start menu select **Programs** (or **All Programs**) > **Websense Email Security** > **QueueView**.

From the Monitor, click  on the Toolbar.

QueueView displays the following information:

Column	What it shows
File Name	The message is stored under this name in the **Out** folder.
Date	The date the message was placed in the **Out** folder.
Time	The time the message was placed in the **Out** folder.
Recipient	The recipient named in the **To** field.
Sender	The sender named in the **From** field.
Subject	The text in the **Subject** field.
Attempts	The number of attempts made to send the message.
Reason for failure	The reason Websense Email Security was unable to deliver the message.

Note

The **Attempts** and **Reason for failure** information is not displayed for Pending or Dead messages.

You can rearrange the QueueView columns by dragging the columns into the order you prefer.

Related topics

- *Resending queued or dead messages*, page 106
- *Deleting a queued or dead email*, page 107

The QueueView Window

QueueView provides descriptive information for 3 types of messages:

Queued message files

If Websense Email Security cannot send an email immediately, it is requeued (see *Requeuing*, page 84).

To view information on a queued message, open **QueueView** and select **View** > **Queued files**. The **Queued Message Files** view is displayed.

Pending message files

Pending messages are email messages that are waiting for Websense Email Security to make an *initial* connection with a mail server so that they can be sent. If Websense Email Security attempts to make a connection but is unsuccessful, the email is queued.

To view information on a pending message, open **QueueView** and select **View** > **Pending files**. The **Pending Message Files** view is displayed.

Dead message files

If Websense Email Security cannot send an email and the total requeuing period has passed, it is designated a dead message. The email file is given a file extension of .d and held in the **Out** folder until you act on it.

To view information on a dead message, open **QueueView** and select **View** > **Dead files**. The **Dead Message Files** view is displayed.

Selecting a type of message to view

To view **Queued** message files, open QueueView and select **View** > **Queued files**.

To view **Pending** message files, open QueueView and select **View** > **Pending files**.

To view **Dead** message files, open QueueView and select **View** > **Dead files**.

Each view is divided into columns showing the following information.

Column	What it shows
File Name	The file name of the email. The email is stored under this name in the **Out** folder.
Date	The date that the email was placed in the **Out** folder
Time	The time that the email was placed in the **Out** folder
Recipient	The recipient in the **To** field.
Sender	The sender in the **From** field
Subject	The subject text in the **Subject** field
Attempts	The number of attempts that Websense Email Security has made to send the email.
Reason for failure	The reason Websense Email Security is unable to deliver the email.

Note

The **Attempts** and **Reason for failure** information is not displayed for Pending or Dead messages.

Click on and drag a column to rearrange the order.

Resending queued or dead messages

You can direct Websense Email Security to make additional attempts to deliver a queued or dead.

1. Open QueueView and select **Queued Message Files** or **Dead Message Files**.
2. Select the message to be resent. Use **Shift** or **Ctrl** to select more than 1 message.

3. Right-click the message and select **Resend Message**.

> **Note**
> When an email is designated a dead message, a failure report is sent to the sender. If you attempt to resend the message and it still cannot be delivered, another failure report is sent. You should therefore avoid resending dead messages unless you are sure that they will be successfully delivered.

4. A confirmation dialog box is displayed. Confirm that you want to resend the selected email.

Deleting a queued or dead email

You can delete queued or dead email. This means that the email is irretrievably deleted and is not sent.

To delete a queued or dead email:

1. Open QueueView and select the view that you want to work with – either **Queued Message Files** or **Dead Message Files**.
2. Select the email to be deleted, right-click and select **Delete Message**.
3. Confirm the action.

You can automatically delete dead messages immediately after the requeuing period has passed. See *Dead Messages*, page 85.

5 Dashboard

The Dashboard is a browser-based application that you can use to monitor the health and status of your Websense Email Security system. You can review:

- Cumulative filtering statistics
- Current system status, covering ThreatSeeker technologies (such as Reputation Service and Anti-Spam Agent), subscription status, connections to external systems, and more
- System alerts, warnings, and informational messages
- Inbound connection activity, inbound filtering, and outbound filtering
- The number of messages in each isolation queue

A complete update of the Dashboard page occurs every 5 minutes, and the following time-sensitive features are refreshed every 20 seconds:

- Alerts, External Systems, Isolation Queues, and Version panels
- In Folder and Out Folder counts at the bottom of the Graphs panel

In addition, the legends for graphs displayed on the page update every 5-10 seconds.

You can also press **F5** to refresh the page at any time.

Related topics

- *Launching the Dashboard*, page 110
- *Using the Value panel*, page 110
- *Using the Alerts panel*, page 111
- *Using the External Systems panel*, page 115
- *Using the connections and filtering graphs*, page 115
- *Using the Isolation Queues panel*, page 117
- *Using the Version panel*, page 117

Launching the Dashboard

To launch the Dashboard from anywhere in the network, open a supported Web browser, and go to:

```
http://<servername>:9090/Dashboard
```

The supported Web browsers are:

- Windows Internet Explorer, Version 7 or 8
- Mozilla Firefox, Version 2 or 3

To launch the Dashboard from the Websense Email Server machine, you can also go to **Start** > **Programs** (or **All Programs**) > **Websense Email Security** > **Dashboard**.

Logging in

A Websense Email Security account is required to log in to the Dashboard. Two levels of Dashboard access are available:

- Dashboard Configuration permissions provide full access to all Dashboard features and settings.
- Dashboard Access permissions permit administrators to view the dashboard, but not to configure alerting behavior or threat groups, or to acknowledge or dismiss alerts.

For information about setting up administrative accounts with the appropriate permissions, see *Configuring administrators for remote access*, page 87.

View preferences

When you configure certain Dashboard features, your preferences are stored in a browser cookie. This means that your preferences are saved for the current browser on the current machine. If you log on to the Dashboard from another machine, the default view is displayed.

The following details are stored in the cookie:

- The size of the Alerts panel (default or expanded)
- Which graphs are displayed
- The time period represented in the graphs
- Which servers are tracked in the graphs
- Whether the graphs are auto- or fixed-scale

Using the Value panel

The **Value** panel, in the top, left corner of the Dashboard, displays information about:

- Inbound and outbound email messages processed (denied, isolated, and allowed) since product installation
- ThreatSeeker components that you have configured

The ThreatSeeker Technology column can show information about: Reputation Service, Anti-Spam Agent, the URL Database, Compliance, and Websense Data Security Suite.

- If a component is not used in any enabled rule, the component name appears in gray.
- If a component is enabled and loaded properly, a green check mark is displayed.
- If there was a problem loading a component, a warning symbol is displayed.

Using the Alerts panel

The **Alerts** panel lists system errors, warnings, and other alert messages, and provides help for investigating and resolving the condition that caused the alert.

When Websense Email Security detects an alert condition, a new alert is added to the Alerts panel. Alerts are sorted:

1. By severity (error before warning, warning before informational alert)
2. By date and time (the most recent error of each severity level appears above older alerts of the same level)

When a new alert is added to the list, the Alerts title bar flashes four times. If you have associated a sound with the alert type (see *Configuring alert behavior*, page 112), the sound is played.

If an alert condition occurs more than once after the associated alert message is displayed, the original alert message is replaced. Any acknowledgement data is removed, and the **Raised** time is set to reflect the most recent occurrence of the condition. This is done to ensure that a network or software component whose status is fluctuation does not cause a flood of alert messages for a single underlying condition.

To expand the Alerts panel to match the width of the Graphs panels below (hiding the Value panel), click the left arrow next to the panel title.

Related topics

- *Responding to an alert*, page 111
- *Configuring alert behavior*, page 112
- *Alert email messages*, page 113
- *Alert conditions*, page 114

Responding to an alert

To help manage alerts, an link appears to the right of the alert summary.

- If you are actively investigating an alert, click **Acknowledge** to let other administrators know that you are working to resolve the alert.

  The alert message is updated to show the login name of the person acknowledging the alert, as well as the date and time that the alert was acknowledged.

- When you have resolved an alert condition, click **Dismiss** to remove the alert from the list.

To acknowledge or dismiss all entries in the Alerts list, mouse over the down arrow symbol (to the left of the "i" icon) and select the appropriate option from the menu.

If your Websense Email Security deployment includes multiple Dashboard instances, when an alert is acknowledged or dismissed in any instance, the alert message is updated appropriately in all other instances.

Click an alert entry to open a window with detailed alert information and troubleshooting steps. The Alert window includes:

- The date and time that the alert was generated (including time zone)
- Who acknowledged the alert
- What condition caused the alert to be generated
- The potential impact of the alert condition
- Steps to solve the problem

At the bottom of the alert window, click a link to access the Websense Knowledge Base, or to print, copy, or email the content of the window.

Note

If you use Mozilla Firefox to access the Dashboard, the **Copy to clipboard** option is not available. You can still use the browser's own copy functionality to copy and paste text from the alert window.

Related topics

- *Configuring alert behavior*, page 112
- *Alert email messages*, page 113
- *Alert conditions*, page 114

Configuring alert behavior

To configure how alert notifications are delivered, and which conditions generate alerts, click the down arrow symbol (to the right of the "i" icon) at the top of the Alert panel, and then click **Configure**.

If your Websense Email Security deployment includes multiple Dashboard instances, alert behavior configured for one instance does not affect alert behavior for other instances. You must configure alerts for each instance separately.

On the Configure Alerts page:

1. To record alert conditions in the Windows Event Log (default), mark the **Notify to Windows Event Log** check box.
2. To send alert messages via email, mark the **Notify to email addresses** check box. The email address field is automatically prefilled with the addresses of users who have Dashboard Administration permissions (see *Remote administration permissions*, page 88). Selecting this check box also activates options in the **Notify by Email** column in the alert level table. Note that if the Send Service is not active, these email alert notifications cannot be sent.
3. For each alert level (**Error**, **Warning**, or **Information**), indicate:
   - Whether the alert is sent via email
   - Whether the alert is displayed on the Dashboard
   - Whether a sound is played when the alert is generated

   If you enable sounds, click **Browse** to locate the sound file to play. Sound files must be in either .wav or .mp3 format. A different sound can be played for each alert level.
4. To generate an alert when the STEMLog Database reaches a specific size, mark the **Log DB Size** check box, and then indicate the maximum size of your Log Database. An alert will be generated if the STEMLog Database reaches 80% of its maximum size.
5. Specify how many messages must be queued up in the **In Folder**, **Out Folder - Pending**, and **Out Folder - Retrying** to generate an alert. The default is 100.
6. Use the **Isolation Queue Increase** field to specify how much of an increase (percentage) in messages in each selected isolation queue will trigger an alert message (default 100%).

   Deselect any queue for which you do not want to receive alert messages.
7. Click **OK** to save your changes and return to the Dashboard.

Related topics

- *Responding to an alert*, page 111
- *Alert email messages*, page 113
- *Alert conditions*, page 114

Alert email messages

There are 2 ways to generate alert email messages:

- Enable email alerts on the Configure Alerts page.
- Manually email alert information from an Alerts pop-up window.

The subject line has 3 sections: the prefix “[WES Alert],” the alert text, and the name of the affected server machines. For example:

```
[WES Alert] Send service has stopped - server: Kofi
```

The email body includes HTML and plain text content, including alert details and troubleshooting information.

Related topics

- *Responding to an alert*, page 111
- *Configuring alert behavior*, page 112
- *Alert conditions*, page 114

Alert conditions

In addition to the alert behavior defined on the Configure Alerts page (see *Configuring alert behavior*, page 112), system alerts are generated when the following conditions are encountered:

- Any of the following services have stopped:

  Receive service
  Send service
  Scheduler service
  Rules service
  Admin service

- An LDAP server, Personal Email Manager, or Report Central is not responding
- STEMLog Database is not responding, or there is a SQL error
- A product or component subscription or trial has expired, or is about to expire
- Unable to update:

  Digital Fingerprinting for Anti-Spam Agent
  Lexi Rules for Anti-Spam Agent
  Real-time Internet Threat Database
  Anti-Virus Agent
  Heuristics for Anti-Spam Agent
  Master Internet Threat Database
  Anti-Virus Malware Scanner

- Anti-Spam Agent, the Internet Threat Database, or a Compliance rule object failed to load
- Data Security Suite is not configured
- An excessive number of connections were denied within a time range
- No email has been received in a specified number of minutes
- A scheduled task failed
- Servers in the cluster are running different product versions

Related topics

- *Responding to an alert*, page 111
- *Configuring alert behavior*, page 112
- *Alert email messages*, page 113

Using the External Systems panel

The External Systems panel provides information about applications and components related but not integral to Websense Email Security. It lists:

- All configured LDAP servers

  If Websense Email Security cannot communicate with any of the configured servers, an error icon appears. Click the icon for detailed information and troubleshooting steps.

- The current size of the STEMLog Database (in Gigabytes)

  When the database size reaches 80 - 100% of maximum, the size is highlighted in yellow. When the size reaches or exceeds 100%, the highlight color changes to red.

  If Websense Email Security cannot communicate with the STEMLog Database, an error icon appears. Click the icon for detailed information and troubleshooting steps.

- Status information for updates to the ThreatSeeker databases

  Click the **Threat Updates** link to open a pop-up message listing the date and time of the most recent successful update to each component database, with version information. Update details are shown for:

  - Anti-Spam Agent (Digital Fingerprinting, Heuristics, and Lexi Rules databases)
  - Internet Threat Database (full and real-time updates)
  - Anti-Virus Malware Scanner
  - Anti-Virus Agent

  If a ThreatSeeker component is out of date, a warning icon appears. Click the icon for detailed information and troubleshooting steps.

In addition, the External Systems panel includes links to Personal Email Manager and Report Central, if installed. If either component is configured, but Websense Email Security cannot communicate with it, an error icon appears. Click the icon for detailed information and troubleshooting steps.

Using the connections and filtering graphs

The central portion of the Dashboard displays up to 3 graphs, showing current and recent Websense Email Security status. Use the **View** drop-down list to determine which graphs appear:

- Connections and Inbound (default)
- Connections, Inbound, and Outbound
- Inbound and Outbound
- Inbound only

Inbound Connections shows the number of connections denied and accepted by the Websense Email Security Receive service. Mouse over a bar in the chart to see precisely how many connections were denied and accepted during the selected period.

Inbound Filtering shows how many of the accepted inbound messages have been delivered (OK) or placed in selected threat groups. Mouse over a bar in the chart to see precisely how many messages were delivered or placed in each threat group during the selected period. Click **Configure** to specify which isolation queues are associated with each threat group, and to customize the colors used in the graph (see *Configuring filtering graph options*, page 116).

Outbound Filtering shows how many outbound messages were placed in an isolation queue. Mouse over a bar in the chart to see precisely how many outbound messages were isolated in the selected period. Click **Configure** to specify which isolation queues are associated with each threat group, and to customize the colors used in the graph (see *Configuring filtering graph options*, page 116).

In addition to selecting which graphs are displayed, you can customize several graph features:

- Use the **Last** drop-down list to determine the period of time shown in each graph (**24 hours** - default, **30 days**, or **1 hour**).
- Use the **Server** drop-down list to determine whether the data shown applies to **All** servers (default), or to a specific server.
- Use the **Scale** options to determine whether a graph scales automatically (default), or whether a fixed scale is used. If you select **Fixed**, also specify the scale (maximum value shown). Spikes in connections or filtered messages may exceed the capacity of a fixed-scale graph. When this occurs, a red box appears around the graph and the columns in the graph are cropped.

In addition, for the Inbound Connection graph, you can set the flicker rate for the legend colors. Use the Inbound Filtering graph **Configure** drop-down list option to access flicker configuration settings.

Underneath the graphs, a small summary bar shows the total number of messages in both In Folder and Out Folder (sorted by Pending, Retrying, and Dead status).

Configuring filtering graph options

You can configure which threat groups are displayed in the Inbound Filtering and Outbound Filtering graphs, and which isolation queues are included within each threat group.

Note that new isolation queues are always placed in the **Other Isolated** group by default (and can then be moved to other groups). Also, the **OK** group is always associated with the color green, and the palette of available colors cannot be changed.

If your Websense Email Security deployment includes multiple Dashboard instances, options set on the Configure Threat Groups page apply only to the current Dashboard instance. You must configure threat group and filtering graph options for each instance separately.

1. Click **Configure** above the legend for the graph that you want to customize.

   On the Configure Threat Groups page, associated pre-defined or custom isolation queues with each threat group.
2. Use the up and down arrow icons to the left of the threat group name to change the position of the group in the list (and, by correlation, on each bar in the chart).
3. Use the **Active** check boxes to add or remove threat groups from the chart.
4. Use the **Name** field to add or edit threat group names.
5. Drag and drop isolation **Queue** names to move them between threat groups.
6. Use the **Flicker** fields to determine how often the threat group's legend entry flashes when a message is added to any queue in the group.
7. When you are finished making changes, click **OK** to return to the Dashboard.

The appropriate chart is updated to reflect the changes.

Using the Isolation Queues panel

The Isolation Queues panel lists all of the Websense Email Security queues (pre-defined and custom), as well as the number of messages isolated in each queue.

If an alert is associated with a queue, an information icon appears next to the queue name. Click the icon for detailed information.

Using the Version panel

The Version panel displays the current Websense Email Security version (including any hotfixes that have been applied), subscription information, and the operating system version.

If your environment includes multiple Websense Email Security versions, an error icon appears and an alert is displayed. Click the error icon for more information.

The subscription summary displays the number of days remaining in the subscription period. Click **Subscription** for to see the status of your Websense Email Security, Anti-Virus Agent, and Virtual Image Agent subscriptions (if applicable). If your subscription does not include a component, or if your subscription has expired or is about to expire, use the links for **Authorized Reseller** or **Sales Representative** to add a component or renew your subscription.

If your subscription has expired, or is about to expire, an error or warning icon appears and an alert is displayed. Click the error or warning icon for more information.

In environments that include multiple Websense Email Security machines, click the operating system entry to list the operating system for each machine.

6 The Rules Administrator

The Rules Administrator is the facility for defining, creating and managing the rules that support your Acceptable Use Policy (AUP). To work effectively with the Rules Administrator you should:

- Configure the Rules Administrator to meet your needs
- Become familiar with the predefined rules and rule groups
- Create your own custom rules using the Rules objects
- Manage and organize rules for optimum performance

See *How Websense Email Security uses rules*, page 123.

Opening the Rules Administrator

To open the Rules Administrator select:

Start > Programs (or **All Programs**) **> Websense Email Security > Rules Administrator**

Rules Administrator components:

The Rules Administrator toolbar, page 120

The Rules panel, page 121

The Rules Object panel, page 122

Rules Administrator tasks:

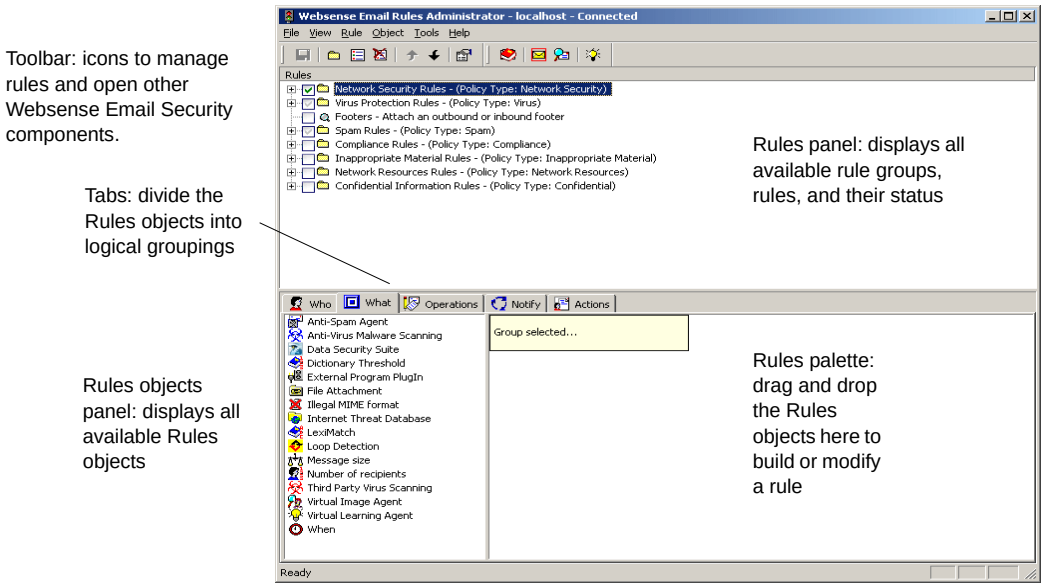
Creating a rule, page 126

Building a rule, page 124

Deleting a rule, page 128

The Rules Administrator window

The Rules Administrator window:



The Rules Administrator toolbar


Save your changes


Create a new rule group


Create a new rule


Delete a rule


Move a rule up the processing order


Move a rule down the processing order


View the properties of a rule


Open Dictionary Management


Open Message Administrator

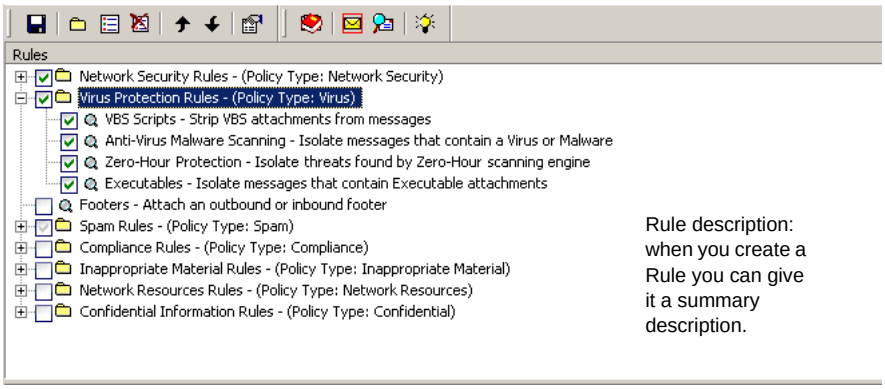

Open the Monitor


Launch Virtual Learning Agent

The Rules panel

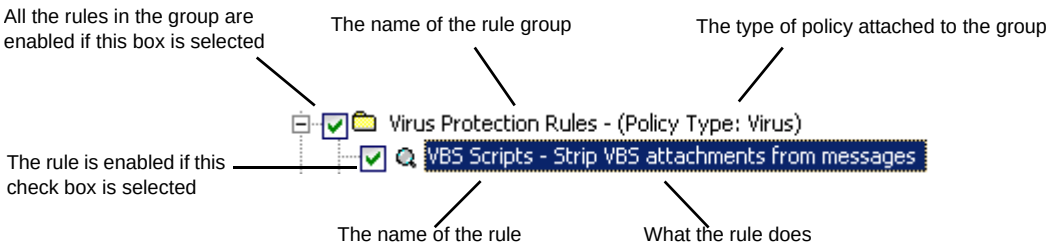
The Rules panel is located in the upper portion of the Rules Administrator window. It displays a list of all the rules that are available, indicating for each whether it is enabled or disabled

The rules are grouped into a logical order. You can create and delete groups, and move rules from one group to another.



Rule description: when you create a Rule you can give it a summary description.

The list items have the following meaning:



Policy type

You can assign a policy type to a group or sub-group from a list of supplied policy types. Policy types are used to identify the category (Confidential, Network Security, Virus, and so on) that an email belongs to and the rule that triggered email blocking. Report Central and Personal Email Manager also use Policy Type to identify the number of messages within specific categories.

To apply a policy type to a rule group:

1. Double-click the rule group or sub-group. A **Properties for <rule group>** dialog box displays.
2. Select a policy type from the drop-down list.
3. Click **OK**.

If you do not assign a policy type to a sub-group, that sub-group inherits the policy type of the group. Also, sub-sub-groups inherit the policy type of the sub-group.

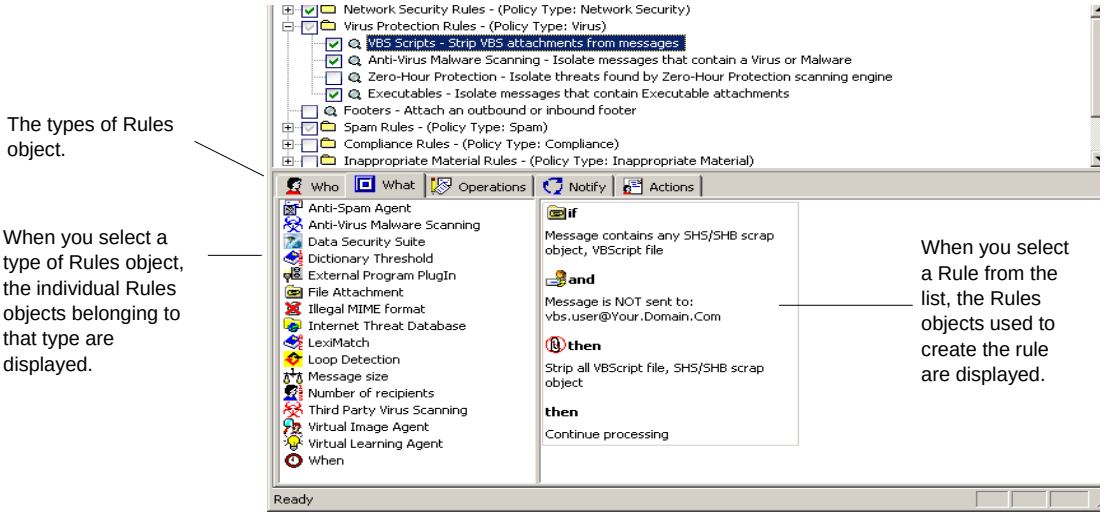
Related topics

- *Predefined rules*, page 129
- *Creating a rule*, page 126
- *Enabling a rule*, page 127
- *Disabling a rule*, page 128
- *Creating a rule group*, page 132

The Rules Object panel

The Rules Object panel is the lower portion of the Rules Administrator window. It includes:

- On the left is the Rules Object pane where the available rules are listed
- On the right is the Rules palette where you build and modify rules



The Rules Object pane

The Rules Object pane is located in the lower left portion of the Rules Administrator window. It lists all of the Rules objects that are available for building a rule.

The Rules Object pane is divided into 5 tabs, 1 for each type of rule object. To build a rule, drag the objects you want to include onto the Rules palette and arrange them in the order you require.

Related topics

- *Rules objects*, page 124
- *The Rules palette*, page 123
- *Building a rule*, page 124

The Rules palette

The Rules palette is located in the lower right portion of the Rules Administrator window. It is the area used to build rules.

To build a rule, drag rule objects from the Rules Object pane, at left, onto the Rules palette.

To configure the object, double click on it.

Related topics

- *The Rules Object pane*, page 122
- *Building a rule*, page 124

How Websense Email Security uses rules

The Rules Service checks the email against the list of enabled rules, starting at the top of the window and working through the enabled rules in order until the email triggers a rule. If an email triggers a rule, Websense Email Security applies the action specified in the rule.

The 4 actions objects – **Allow**, **Delay**, **Discard**, and **Isolate** are *terminating actions*. When Websense Email Security performs a terminating action on an email, no further processing takes place. If an email passes all the rules checks without being isolated, delayed or discarded, it is placed in the **\Out** folder for delivery to its destination.

Rules objects

Rules objects are the basic units you use to create a rule. Starting with the Who object, the table below describes the types of Rules objects and the logical order in which they should be added to a rule.

Type of Rule object	Description
Who objects, page 141	A **Who** object in a rule affects who the rule applies to. For example, an individual, a department, senders or recipients of email. If you do not include a Who object in a rule, the rule will apply to everybody sending and receiving email in and out of your protected domain.
What objects, page 149	A **What** object in a rule checks the characteristics of the email against the criteria you specify – for example size, content, type of attachments.
Operations objects, page 181	An **Operations** object in a rule modifies the email in some way – for example by adding a footer.
Notify objects, page 189	A **Notify** object in a rule causes an email to be sent to the users you specify to notify them that a rule has been triggered.
Actions objects, page 193	An **Actions** object in a rule performs an action on the email, for example isolating it. When an action has been carried out, no further processing takes place on the email.

Building a rule

To build an effective rule, follow these guidelines:

- Begin with a **Who** object.
- Work through the object types in the order they are shown on the **Rules Object** panel:

  Who > What > Operations > Notify > Actions

  You do not have to include every object type in every rule, but without a **Who** or **What** object, every email will trigger the rule.
- Finish with an **Action** object.

Before you build a rule you must create it. See *Creating a rule*, page 126.

Building a Rule:

1. Click the rule that you want to build.
2. Select the **Who** tab. The available Who objects are listed.
3. Select a Who object and drag it onto the Rules palette. The properties sheet for the object displays. Specify the exact conditions of the object.

You do not have to use a Who object in all the rules you create. If you want a rule to apply to everybody sending email to or from your organization, leave out the Who object.

4. When you have configured the Who object, click **OK**. You will see the Who object displayed in the Rules palette.
5. A Continue Processing object is automatically added to the end of the logic block. This remains until you select an Action object to specify how Websense Email Security will deal with email that triggers the rule.
6. Select the **What** tab. Select a What object to specify the criteria to be applied. All available What objects are listed.
7. Drag a What object onto the Rules palette and place it underneath the Who object. The properties sheet for the chosen What object displays.
8. Configure the What object and click OK. The What object displays under the Who object.
9. Add more objects to develop your rule. These could be from the **What**, **Operations**, or **Notify** tabs. You do *not* have to use an object from each tab.
10. When you have finished building the rule you can enable it. Make sure the check box for the rule is selected.
11. Click  to save your changes. The new rule is not applied to any email until the rule has been saved.

Related topics

- *Rules objects*, page 124
- *Who objects*, page 141
- *What objects*, page 149
- *Operations objects*, page 181
- *Notify objects*, page 189
- *Actions objects*, page 193
- *Creating a rule*, page 126

Connecting Rules objects

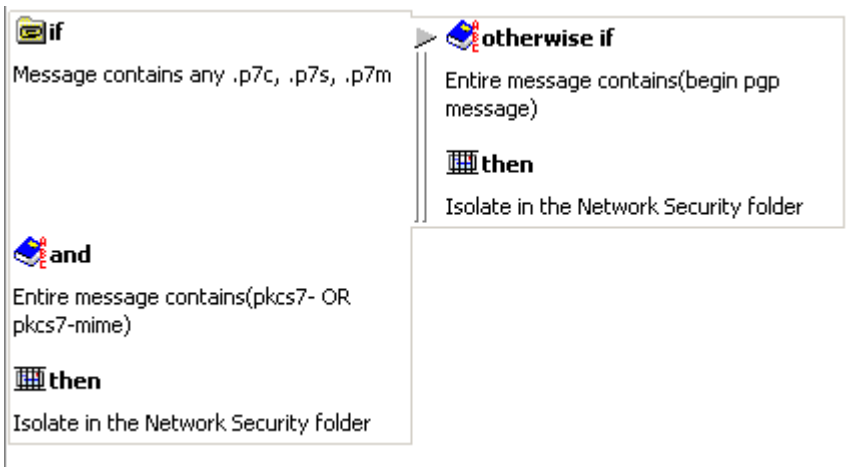
You can connect Rules objects together in different ways, depending on how you want the rule to work. Rules objects connected together form logic blocks, and you can connect these logic blocks to form a complete rule.

The logical connections are:

Connector	What it does
IF	The opening statement of a rule.
AND	Adds extra conditions to the logic block.

Connector	What it does
OTHERWISE IF	Creates a new logic block that will trigger if the conditions of its preceding logic block are not met.
THEN	Connects the conditions to an event that will take place if the conditions are met – a **Notify**, **Operations** or **Action** object.

For example, this rule has 2 logic blocks and uses all 4 connectors.



Creating a rule

When you create a rule, the procedure is the same for any rule and any Rules object.

To create a rule:

1. Open the Rules Administrator.
2. Right-click any rule in the Rules description area. A shortcut menu displays.
3. Select **New Rule** . The **Properties for New rule** dialog box displays.
4. Enter the name of the rule and a brief description of what the rule does.
5. To enable the rule immediately, select the **Enabled** check box.

> **Note**
> The rule is not applied to email until you save your changes.

6. Click **OK**. The Rules palette is cleared. You can now add Rules objects.
7. Select the tab for the type of Rules object. The individual Rules objects are displayed in the tab.
8. Select a Rules object from the list and drag it onto the Rules palette.
9. In the dialog box for the Rules object, set the conditions.

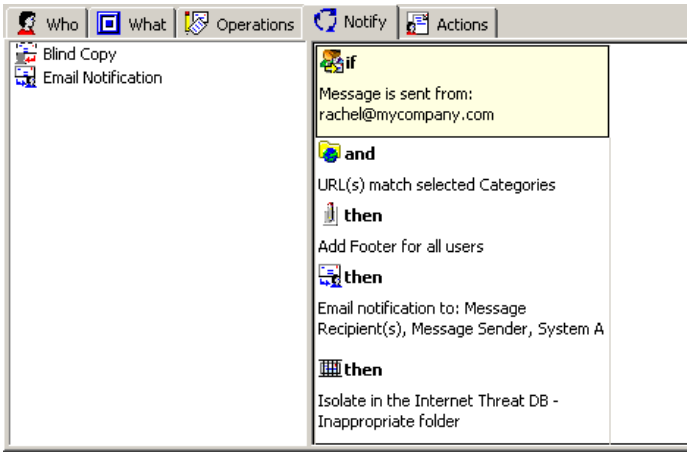
To learn more about Rules objects and how to configure them, see *Rules Objects*, page 141.

> **Note**
> You do not have to use a Who object in all the rules you create. For example, if you want a rule to apply to everybody sending email to or from your organization, do not use the Who object.

10. Click **OK**.

    A **Continue Processing** object is automatically added to the end of the logic block, and remains there until you select an Action object that specifies how Websense Email Security will deal with email messages that trigger the rule.

    Add further objects to develop your rule as needed.



11. If you did not select to enable the rule when you were creating it, enable it now by selecting the check box next to the rule.
12. Click  to save your changes.

> **Note**
> Your rule is not applied to email until you save your changes and enable the rule.

Enabling a rule

To enable a rule:

1. In the Rules Administrator window, check the box next to the rule you want to enable.
2. Click  to save your changes.

> **Note**
> The rule is not applied until the change is saved.

Disabling a rule

To disable a rule:

1. In the Rules Administrator window, clear the check box next to the rule you want to disable.
2. Click  to save your changes.

> **Note**
> The rule is not disabled until the change is saved.

Deleting a rule

To delete a rule:

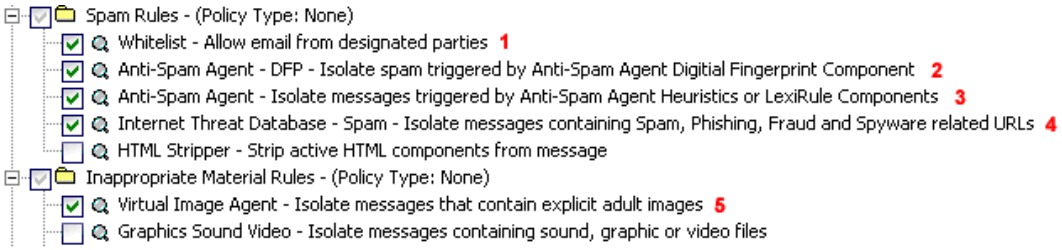
1. In the Rules Administrator window, select the rule.
2. Click  .
3. Confirm that you want to delete the rule.
4. Click  to save your changes.

> **Note**
> If you do not save your changes, the rule continues to be applied.

Positioning of rules

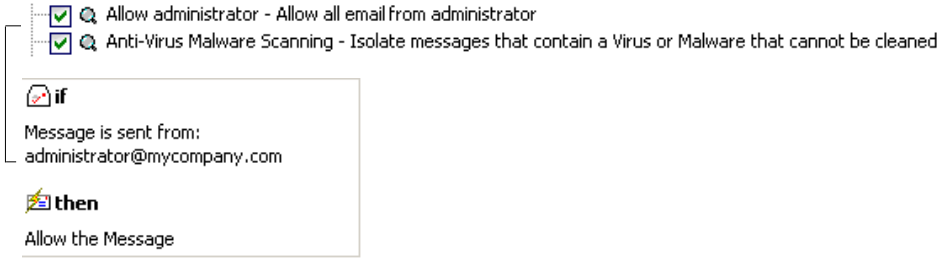
When Websense Email Security processes an email, it checks the email against each of the rules in order, from the top of the screen until it reaches a terminating action (Allow, Delay, Discard, or Isolate) or until the all the email has been checked against all the rules and allowed to continue. Changing the order of rules can therefore change which messages trigger rules and which are allowed to reach their destination.

Rules are always processed from the top of the screen to the end, regardless of the Rule Group they are in.



When an email triggers a rule with an Action object (Allow, Delay, Discard, or Isolate) it is not checked against any subsequent rules.

In the example below, the user has made the mistake of placing a rule allowing all email from the systems administrator above a rule to detect virus-infected email.

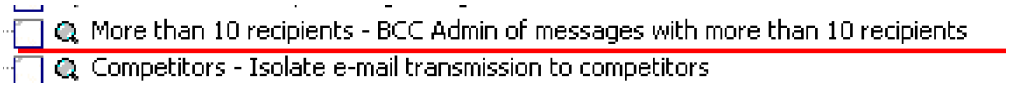


This means that if the administrator were to send a virus-infected email, it would be checked by the first rule and allowed to continue without any further processing. The email would not be checked against the Anti-Virus Malware Scanning rule because it had already encountered a terminating action (the Allow object in the first rule).

Moving rules

Use the arrow buttons   to move a selected rule up or down the order.

Alternatively, use the mouse to drag the rule into position. A red line indicates where the rule will be placed.



Predefined rules

Websense Email Security is supplied with a comprehensive set of predefined rules that enable you to start filtering email immediately.

Although the predefined rules are a quick and easy way to begin filtering email, you still need to enter some details to make the rules work correctly in your organization. For example, you need to enter your domain name in the Footers & Banners rule, and specify the location of your anti-virus scanning software for the Virus rule.

Rule Group	Rule	What it does
Network Security Rules	Loop Detection	Isolates email that loops more than 5 times.
	Illegal MIME format	Isolates non-standard or malformed email.
	Encrypted	Detects if staff are transmitting S/MIME or PGP files.
	Compressed	Isolates mail that fails automatic decompression.
	Encryption gateway	Redirects mail to the specified Smart Host server for encryption

Rule Group	Rule	What it does
Virus Protection Rules	VBS Scripts	Strips VBS attachments from email.
	Anti-Virus Malware Scanning	Isolates email that contains a virus or malware that cannot be cleaned.
	Internet Threat Database Real-Time Protection	Isolates virus threats found by ThreatSeeker real-time URL categorization
	Executables	Isolates email that contains executable attachments.
	Footers	Attaches an outbound or inbound footer.
Spam Rules	Whitelist	Allows email from designated parties.
	Anti-Spam Agent - DFP	Isolates email that triggers the Anti-Spam Agent Digital Fingerprinting component.
	Anti-Spam Agent	Isolates email that triggers the Anti-Spam Agent Heuristics or LexiRules components.
	Internet Threat Database - Spam	Isolates email from the database that contains spam-, phishing-, fraud- or spyware-related URLs.
	HTML Stripper	Strips active HTML components from email.
Compliance Rules	HIPAA Compliance	Isolates email that contains individually identifiable health information. Relates to the Health Insurance Portability and Accountability Act regarding the security and privacy of health data.
	GLBA Compliance	Isolates email that contains financial information. Relates to the Gramm-Leach-Bliley Act regarding the personal financial information held by financial institutions.
	PCI Compliance	Isolates email that contains payment card information.
	State Data Privacy Laws	Isolates email that contains Social Security Numbers.
Inappropriate Material Rules	Virtual Image Agent	Isolates email that contains explicit adult images.
	Graphics Sound Video	Isolates email containing graphics, sound or video files.
	Adult Dictionary	Isolates email with an Adult dictionary score > 100.
	Gambling Dictionary	Isolates email with a Gambling dictionary score > 100.
	Offensive or Derogatory	Isolates email with Hate or Violence Dictionary.
	Internet Threat Database - Inappropriate	Isolates email that contains inappropriate URLs, which are listed in the ITD.

Rule Group	Rule	What it does
Network Resources Rules	Files > 5MB	Automatically compresses email larger than 5 MB.
	Files > 2MB	Delays email larger than 2 MB.
	More than 10 recipients	Blind copies the administrator if email has more than 10 recipients.
Confidential Information Rules	Competitors	Isolates email transmission to competitors.
	Computer Security	Isolates outbound email containing the word “username” or the word “password”.
	Confidential Information	Isolates outbound email containing intellectual property or confidential data.
	Websense Data Security Suite Inspection	Sends outbound messages to Websense Data Security Suite for inspection and isolates messages returned with the “block” recommendation.

Enabling predefined rules

1. In the Rules Administrator window, to enable a rule select the check box next to its name.
2. If the rule must be configured, the **Rule Configuration wizard** automatically starts. Click **Next** and follow the instructions in the wizard.

Note

If you enable a rule but don’t complete the Rule Configuration wizard, the rule may not filter email correctly.

Editing predefined rules

Clicking a rule causes its objects to be displayed in the Rules palette. You can edit predefined rules to suit your needs in the same way that you create a new rule.

See *Building a rule*, page 124 to find out more about how to create rules. See *Rules objects*, page 124 for a complete list of Rules objects.

Rule groups

You can organize your rules by moving them into groups. Rule groups make it easier to manage and apply your rules, so that you can:

- Keep similar rules together
- Enable all similar rules with a single mouse click, for example all the anti-spam rules.

- Quickly and easily delete a rule set you no longer need.

The predefined Websense Email Security rules are organized into 5 groups (see *Rules objects*, page 124).

Related topics

- *Creating a rule group*, page 132
- *Moving a rule into a group*, page 132

Creating a rule group

To create a rule group:

1. Open the **Rules Administrator**.
2. Select **Rule** > **New Group** or click  . The **New Group** dialog box displays.
3. Enter a name for the group.
4. To create a new rule within the new group, select **Create a New Rule**.
5. Click **OK**. The new group displays in the Rules panel.

If you selected **Create a New Rule**, the **New Rule** dialog box displays automatically. The new rule you create is automatically placed inside the group that you created.

Moving a rule into a group

To move a rule into a group, click the Rule you want to move and drag it onto the group. When the mouse pointer is positioned correctly over a rule, the pointer becomes a red arrow. If you release the mouse button, the rule becomes part of that group.

Working with groups of rules

Note

You must save your selected rules to be able to activate them.

You can enable or disable a group of rules, or enable or disable 1 or more rules within a group.

Enabling a group of rules

You can enable all the rules in a group by selecting the check box of the group. All the rules in the group are selected automatically.

Disabling a group of rules

Clear the check box next to the group to disable all the rules in the group.

Enabling rules within a rule group

If you do not select all of the rules in a group, the group check box is shown grayed to indicate that the group is partially selected.

Exporting rules

You can export rules into a separate **.rul** file, which you can then use to restore your saved rule set. This is valuable if you are deploying Websense Email Security on multiple servers, if you are undertaking server maintenance and want to keep your current rule configuration in place, or if you want to make a backup of your rules.

To export your rules to a .rul file:

1. In the Rules panel, select the Rules to export. You can select any number of rules or groups, or the entire rule set.

   Note
   When you export a rule group, all the rules within that group are exported.

2. Select **File** > **Export Rules**. The **Save As** dialog box displays.
3. Save your .rul file in the required location.
4. Click  .

   A confirmation message displays when Websense Email Security has successfully exported the rules.

Importing rules

You can import a **.rul** file containing Websense Email Security Rules.

Note
If a rule you are importing already exists in the Rule panel, Websense Email Security adds an additional copy. Importing a rule does not overwrite any of your current rules.

You can:

- Import a rule set that you have previously exported

- Import the same rule set onto each server running Websense Email Security in your organization
- Restore the default rule set included in the Websense Email Security install

To import a .rul file into Websense Email Security:

1. From the **File** menu, select **Import Rules**. The **Open** dialog box displays.
2. Select the .rul file you want to import and click **Open**. The **Import Rules** dialog box displays. It displays a list of rules that the .rul file contains.
3. Select the rules to import. If you select a rule group, all the rules in that group are imported.
4. Specify where you want the selected rules to be placed in the Rules panel:
   - **Insert after the selected rule** –The imported rules are placed after whichever rule is currently highlighted in the Rules panel.
   - **Insert after the last rule** – The imported rule are placed at the end of the list of rules.
5. Click **Import**. The imported rules are displayed in the Rules panel.

Configuring the Rules Administrator

The Rules Administrator configuration settings affect the way email is checked against the Rules, and can affect the speed with which email proceeds through the rules checking process.

Rules Administrator configuration settings:

Setting	What it does
Dictionary Scanner	Dictionary scanning: • Specifies which files are scanned against the dictionaries for content that could trigger a rule. • Specifies how much of each file is scanned.
Password Protected Archives	Sets up decompression of encrypted and password protected files.
Document	Set up the extraction of data from compound document files, so that Websense Email Security can check them against the rules. See *Document decomposition*, page 297.
HTML Parser	Set up the parsing of HTML email to combat HTML spam.
DSS Settings	Register, deregister and set error handling options for the Websense Data Security Suite server.

Configuring dictionary scanning

Many rules check the contents of an email and its attachments against the Websense dictionaries. However, some file types are more suitable for dictionary scanning than

others. To save processing time, you can select not to scan certain file types, for example, image or audio files, or to only scan a specified amount of each email.

To configure dictionary scanning:

1. In the Rules Administrator, select **Tools** > **Options**. The **System Options** dialog box displays.
2. Select the **Dictionary Scanner** tab.
3. Specify how much of each email is to be scanned against the dictionaries:

   Default = 10KB

   Maximum =10,000KB.

   The greater the scanning size, the longer it takes to check large messages against the rules.
4. Select the file types are to be exempt from dictionary scanning. You can select groups of file types, for example audio files, or specific file types, for example, MP3s.
5. To add a file type to the list, click **Add extension**. Enter the file type in the text box.

   Note
   Do not include the period (“.”) character. For example, enter “txt”, not “.txt”.

6. To remove a file type you added, select it and click **Remove extension**.

   Note
   You cannot delete the preset file extensions.

7. Click **OK**.

Configuring password protected archives

You can prevent unauthorized users and domains from receiving password protected archive files, such as a zip file with a password, by entering recipient/password pairs on the **Password Protected Archives** tab.

You can specify which users are allowed to receive password protected archive files, and the password that was used to create these files. Websense Email Security uses the password to decompress the file and scan the contents. If a user that has not specified a password is sent an email with a password protected archive file, or is sent a password protected file with a different password, the email will trigger the predefined rule, if enabled.

To add a recipient/password pair:

1. In the Rules Administrator select **Tools > Options.** The **System Options** dialog box displays.
2. Select the **Password Protected Archives** tab.

3. Click **Add**. The **Enter Recipient/Password Pair** dialog box displays.
4. In the **Recipient/Domain** text box, enter the name of the recipient or domain to add.
5. If you are using Windows authentication, you can find recipients or domains by clicking **Browse**.

> **Note**
> If you are using SQL authentication, **Browse** is not available. See Websense Knowledge Base Article 1294. It provides details of when and how to use the authentication methods.

The **Select Users** dialog box displays. You can select to retrieve the following users:

- Monitored External users
- Monitored Internal users
- Imported users/groups database
- Windows address book
- Outlook address book

6. Select which user you want to retrieve from the **Select users from** drop-down menu and click **Add**.

Retrieving recipients using LDAP

If you are using Windows authentication, you can also retrieve a list of recipients or domains using an LDAP connection.

1. If you have already configured a connection to the LDAP server, the connection is listed in the **Select users from** drop-down menu.
2. The recipients retrieved are displayed in the user list. To add a user, select the user and click **Add**.
3. After you add the user, click **OK**. The user name or email address displays in the **Recipient/Domain** text box.

To configure a connection to the LDAP server:

1. Click **LDAP** and configure the connection. See *Configuring an LDAP connection*, page 146.

Configuring Document Decomposition

Websense Email Security can extract data from supported files and apply the current filtering rules to that data. You can decompose documents and then:

- Scan extracted text with the Dictionary Scanner object
- Examine extracted pictures with the Virtual Image Agent object
- Detect executables that are embedded in a file

- Scan extracted files with the Anti-Virus Agent Malware Scanning object

By default, decomposition of all documents is enabled. Websense Email Security can decompose nested and combined containers with up to 25 levels of depth. For example, a Word document inside a Zip container that is inside an Excel workbook.

To enable document decomposition:

1. Open the **Rules Administrator** and select **Tools > Options**. The **System Options** dialog box displays.
2. Select the **Document Decomposition** tab.
3. Select **Enable document decomposition**.
4. Click **Advanced**. The **Advanced Properties** dialog box displays.
5. Select the document types from which to extract data. For more about file decomposition, see *Choosing files for decomposition*, page 137.
6. Click **OK**.

Choosing files for decomposition

You can specify which document categories and types will be decomposed.

- Database Formats
- Desktop Publishing Formats
- Email Formats
- Embedded Formats
- Other Formats
- Presentation Formats
- Spreadsheet Formats
- Word Processing Formats

For a full list of the types that Document Decomposition supports, see *Document decomposition*, page 297.

To select the file types to be decomposed:

1. Open **Rules Administrator** and select **Tools > Options**. The **System Options** dialog box displays.
2. Select the **Document Decomposition** tab.
3. Click **Advanced**. The **Advanced Properties** dialog box displays.
4. Select the document types you want document decomposition to extract data from.
5. Click **OK**.

Configuring HTML parsing

A common spamming technique uses HTML tags to break up the flow of text to defeat anti-spam filters.

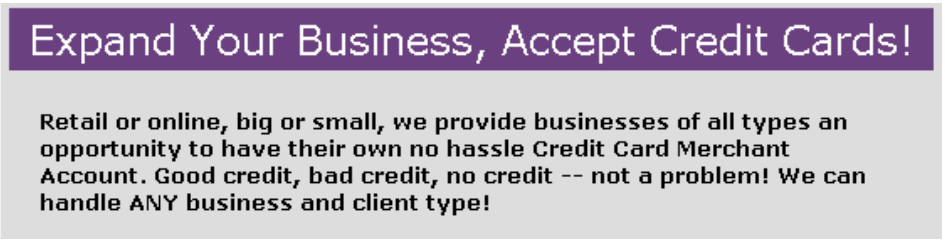
The HTML Parser extracts the user-visible text from the HTML document so that it can scanned by the Dictionary Scanner. User-visible text is text that is visible to the user, as opposed to white-on-white text, text in hidden HTML tags, or text outside the valid parts of an HTML document.

> **Note**
> As well as extracting visible text, the HTML parser extracts URLs from the body of the email into a text file called SC_URL.txt. You can examine this file in Message Administrator.

There are 2 types of HTML parsing that can be enabled. By default, both are enabled.

- HTML extraction from email body – This extracts the user-visible text from the email body so that the text can be scanned.
- Text extraction from HTML attachments – This extracts text from HTML attachments so that the text can be scanned.

For example, here is the body of an HTML spam email.



Here is a section of source code from the same email:

```
<B>Re<!KQ>ta&#105;l or onl&#105;ne, b&#105;g or small, &#119;e
prov&#105;de bus&#105;nesses o<!NJ>f all <!KQ>t<!HOM>ypes an
oppor<!KQ>tun&#105; <!KQ> t<!HOM>y <!KQ> to have <!KQ>
the&#105;ro&#119;n no hassle Cred&#105;<!KQ>t Card Merchan<!KQ>t
Accoun<!KQ>t.
```

The spammer has inserted HTML tags into the middle of words to avoid detection. When the HTML Parser is enabled, the HTML tags are removed so that the remaining text can be scanned by the dictionary scanner.

To enable HTML parsing:

1. Open the Rules Administrator and select **Tools > Options**. The **System Options** dialog box displays.
2. Select the **HTML Parser** tab.
3. Select the types of HTML parsing to apply to email. By default, both are enabled.
4. Click **OK**.

Configuring the Data Security Suite connection

If your organization uses Websense Data Security Suite and you want to use a rule that interfaces to Data Security Suite to perform compliance inspection, you must register the Data Security Suite server and select an error handling option.

To register the Data Security Suite server with Websense Email Security:

1. In the Rules Administrator go to **Tool** > **Options** and select the **DDS Settings** tab.
2. Click the **Register DSS Server** button. The **Register DSS Server** dialog box displays.
3. Enter the name of the Data Security Suite server and the DSS user name and password. Click **Register**. Websense Email Security attempts to register with the DSS server.

   If registration is successful, a message displays indicating success. This message also includes the following information:

   ```
   To deploy the DSS policy:
      1. Go to DSS Manager > Configuration, and click the
         flashing Deploy Settings button.
      2. Go to DSS Management Console and adjust policy to use
         the new Websense Email Security channel.
      3. In Websense Email Security, go to Rules Administrator
         and enable the Data Security Suite rule.
   ```

   On the **DSS Settings** tab, the Register DSS Server button is disabled and the Deregister DSS Server is enabled.

   If registration fails, an error message indicates the cause of the failure. Correct the problem indicated by the error message and perform the registration steps again.
4. Specify how to handle messages that fail Data Security Suite processing. Select one of the following options:
   - Continue processing
   - Copy to folder and continue processing
   - Copy to folder and stop processing

   Selecting either of the “Copy to folder...” options causes an entry field and Browse button to display. Enter the name and path of a folder or click Browse to locate and select a folder. The default location is the **\Out** folder. In a typical installation the location is: C:\Program Files\Websense Email Security\Out\.
5. Click **OK**.

To deregister the DSS server, click **Deregister**.

To use Data Security Suite with a proxy server, open Secure Sockets Layer on port 8443 on your proxy server.

To use the Data Security Suite object in a rule, see *Configuring the Data Security Suite object*, page 159.

7 Rules Objects

Websense Email Security does its work by checking email against a set of rules that you specify. If the Rules Service detects that an email has triggered a rule, that email is disposed of as specified by the rule.

Rules objects are the logical units used to create a rule. There are several rules objects. For a list and description of each, see *Rules objects*, page 124.

For a description of the Rules Administrator and information about building rules, see *The Rules Administrator*, page 119.

The presentation of each Rules object includes a description of:

- The purpose of the object
- How to configure the object
- The effects of using reverse logic with the object

Related topics

Who objects, page 141
What objects, page 149
Operations objects, page 181
Notify objects, page 189
Actions objects, page 193

Who objects

A **Who** object checks the sender, recipients or the direction of email. If you do not specify a **Who** object in a rule, the rule applies to every email sent to or from your protected domain.

The **Who** objects include:

- *From Users and Groups object*
- *Inbound/Outbound Mail object*
- *To Users and Groups object*

From Users and Groups object

The **From Users and Groups** object checks the contents of the email messages **From** field against criteria that you specify. Websense Email Security checks whether or not the email comes from a specified email address, group or domain.

Configuring the From Users and Groups object

To configure the **From Users and Groups** object:

1. Drag the **From Users and Groups** object onto the Rules palette. The **Properties for From Users and Groups** dialog box displays.
2. **Message senders** – Click either:
   - **Add** – To manually enter addresses for users or domains. See step 3.
   - **Browse** – To select addresses for users or groups from a data source. See *Retrieving user information from a data source*, page 144.
3. If you clicked **Add**, the **Add Senders** dialog box displays. Enter 1 or more users, groups or domains. Separate multiple entries with a semicolon.
4. Click **OK**. The senders are displayed in the **Message senders** list.

    = Individual user

    = Group of users

    = Domain
5. Click **OK**. The users and groups are displayed in the Rules palette.

Reverse Logic – If you select the **Reverse logic** check box, the rule is triggered if the email is *not* from the user, group or domain that you specify.

Related topics

- *Retrieving user information from a data source*, page 144

Inbound/Outbound Mail object

Warning

If you enable a rule that contains the Inbound/Outbound Mail object, you must have anti-spoofing enabled somewhere in your system, either in the Receive Service (see *Anti-Spoofing*, page 41) or with an upstream MTA. Without anti-spoofing there is a risk that spoofed inbound mail will be treated as internal.

The Inbound/Outbound Mail object specifies whether a rule applies to email coming into, going out of, or coming from within the protected domain. This avoids unnecessary email processing. For example, you can apply anti-spam filtering only to email coming into your organization.

The Inbound/Outbound Mail object checks the domain of the email sender and the domain of the email recipient against the criteria you specify.

Option	What it does
Inbound	The rule applies only to email sent from *outside* a protected domain to a recipient *inside* a protected domain.
Outbound	The rule applies only to email sent from *inside* a protected domain to a recipient *outside* a protected domain.
Internal	The rule applies only to email sent from *inside* a protected domain to a recipient *inside* a protected domain.
External Relay	The rule applies only to email sent from *outside* a protected domain to a recipient *outside* a protected domain.

Configuring the Inbound/Outbound Mail object

1. Drag the Inbound/Outbound Mail object onto Rules palette. The **Properties for Inbound/Outbound Mail** dialog box displays.
2. Select the types of email the rule will apply to. Any or all can be selected.
3. Select the protected domains to include in the rule. By default, the rule checks against all protected domains. To use only specific domains, click **Selected** and then select 1 or more of the protected domains in the list.
4. To reverse the logic, select the **Reverse logic** check box.
5. Click **OK**.

Reverse logic – Inbound/Outbound Mail object

The table describes the results of selecting **Reverse logic** for the Inbound/Outbound Mail object. The example uses the protected domain **mycompany.com**.

Message type	Result
Inbound	The rule is triggered if the email is sent from: • **Inside** mycompany.com to **any recipient**. • **Outside** mycompany.com to a recipient **outside** mycompany.com
Outbound	The rule is triggered if the email is sent from: • **Outside** mycompany.com to any recipient. • **Inside** mycompany.com to a recipient **inside** mycompany.com
Internal	The rule is triggered if the email is sent from: • **Outside** mycompany.com to **any recipient**. • **Inside** mycompany.com to a recipient **outside** mycompany.com
External Relay	The rule is triggered if the email is sent from: • **Outside** mycompany.com to a recipient **inside** mycompany.com • **Inside** mycompany.com to a recipient **outside** mycompany.com • **Inside** mycompany.com to a recipient **inside** mycompany.com

To Users and Groups object

The **To Users and Groups** object checks the contents of the **To** field of an email against criteria that you specify. Websense Email Security checks to see if the email is addressed to a specified email address, group or domain.

Configuring the To Users and Groups object

1. Drag the **To Users and Groups** object onto the Rules palette. The **Properties for To Users and Groups** dialog box displays.
2. **Message recipients** – Click either:
   - **Add** – To manually enter addresses for users or domains. See step 3.
   - **Browse** – To select addresses for users or groups from a data source. See *Retrieving user information from a data source*, page 144.
3. If you clicked **Add**, the **Add Recipients** dialog box displays.
4. Enter 1 or more users, groups or domains. Separate multiple entries with a semicolon.
5. Click **OK**. The senders are displayed in the **Message recipients** list.

    = Individual user

    = Group of users

    = Domain
6. Click **OK**. The users and groups that you added are displayed in the Rules palette.

Reverse Logic – If you select the **Reverse logic** check box, the rule is triggered if the email is not to the user, group or domain that you specify.

Retrieving user information from a data source

As well as entering user details manually in a Rules object, you can also retrieve a list of users, groups or domains from your system. The advantages of this are:

- You can add multiple users, groups or domains at one time
- You do not have to remember user details
- You remove the risk of misspelling user details

The following methods automatically retrieve user information.

Data source	Details
Monitored external users	Every time an email from outside the protected domain triggers a rule, Websense Email Security collects the details in the logging database. You can retrieve a list of these addresses to use in **Who** rules.
Monitored internal users	Every time an email from inside the protected domain triggers a rule, Websense Email Security collects the details in the logging database. You can retrieve a list of these addresses to use in **Who** rules.
Imported Users/Groups database	If you created a users/groups database using the ScoutGroupDB, you can retrieve the users and groups details from there. For details of how to create a database of users and groups, see the *Websense Email Security Installation Guide*.
Windows address book	Retrieve user details from the Windows address book.
Outlook address book	Retrieve user details from the Outlook address book.
LDAP	Retrieve user details from the LDAP server. To retrieve user details using LDAP, you must first configure a connection to the LDAP server, see *Configuring an LDAP connection*, page 146.

To retrieve a list of users:

1. Drag the relevant Who object onto the Rules palette. The object's dialog box displays.
2. Click **Browse**. The **Select Users** dialog box displays.
3. Select the data source from the drop-down list.
   - Monitored external users
   - Monitored internal users
   - Imported Users/Groups database
   - Windows address book
   - Outlook address book.
   - LDAP connection

     To retrieve user details from the LDAP server, you first need to configure a connection to the LDAP server. See *Configuring an LDAP connection*, page 146.

   The user details are displayed in the left pane.
4. Select users, groups and domains and click **Add**.
5. To remove a user, group or domain, select it and click **Remove**.
6. When you have chosen the users and groups to include in your Who rule, click **OK**.

Configuring an LDAP connection

To use LDAP to retrieve user details, set up a connection to the LDAP server.

1. Click **LDAP** in the **Select Users** dialog box. The **LDAP Connection** dialog box displays.
2. Click **Add**. The **Add LDAP Connection** dialog box displays. It has 2 tabs:
   - General (*Add LDAP Connection - General tab*)
   - Advanced (*Add LDAP Connection - Advanced tab*)

After configuration, if the LDAP connection is working, when you select the LDAP connection, users and groups are retrieved from the LDAP server and displayed in the left pane of the dialog box. You can include these users and groups in any Who rule.

If the users and groups do not display, see *Testing the LDAP connection*, page 147.

Add LDAP Connection - General tab

In the General tab, enter the details of the LDAP server:

1. Enter a name for the connection. This is the name displayed in the **Select Users From** dialog box when you browse for users and groups to include in a Who object. See *Retrieving user information from a data source*, page 144.
2. In the **Server name** field, enter the name of the LDAP server from which you want to retrieve information.
3. To make it compulsory that Websense Email Security use a username and password to log on to the LDAP server, select **Log on to the server**, and then enter the username and password.

   To connect to the LDAP server anonymously, clear the **Log on to the server** check box.
4. If you want Websense Email Security to connect to the LDAP server using secure authentication, select **Log on using Secure Authentication**.
5. Select the **Advanced** tab to complete the configuration. See *Add LDAP Connection - Advanced tab*.

Add LDAP Connection - Advanced tab

In the Advanced tab:

1. Enter the LDAP port number of the LDAP server.

   Default = 389

   If you want to connect to the LDAP server using a secure connection (Secure Sockets Layer), select **Use a secure connection (SSL)**. If you enable SSL, the default port number becomes 636.

2. Specify a search base for the LDAP query. The search base is the starting point for the query. LDAP users and groups information is not stored on the Websense Email Security server; it is requested from the LDAP server when necessary, so specifying a search base makes the connection more efficient at locating specific users or groups.
   - To automatically enter the default search base, click **Get Default**.
   - To manually specify a search base, click **Specify Group Object**. The **LDAP Server Options** dialog box displays.

     By default, Websense Email Security uses the default group object, GroupofNames. To specify a different Group object, for example, “sales”, enter the name in the text box.
3. Click **OK**.

If you have successfully configured the LDAP connection, it is prefixed by LDAP in the **Select users from** drop-down list in the **Select Users** dialog box.

The users and groups retrieved from the LDAP server are displayed in the list.

If the users and groups are not displayed successfully, you can test the LDAP connection.

1. Click the **General** tab on the **Add LDAP Connection** dialog box.
2. Click **Test Connection**. See *Testing the LDAP connection*.

Testing the LDAP connection

You can test Websense Email Security connectivity to the LDAP Server.

The process includes 3 tests, run in the following order:

1. Test Basic LDAP connection
2. Test LDAP Authentication
3. Test Search for Groups and Users

Basic LDAP connection test

The basic LDAP connection test fails if Websense Email Security cannot make a TCP/IP connection with the server. If the test fails, a dialog box displays the details.

Make sure you have specified the server name or IP address and LDAP Port number correctly. The server may not use the default port number of 389. If the server and port number are correct, other possible causes of a connection failure include:

- The server is not running
- The server is running but its LDAP service is not
- There is a firewall or DNS block or misconfiguration

Test LDAP Authentication

The LDAP Authentication test fails if the LDAP server cannot authenticate your user details (username, password and domain name). If the test fails, a dialog box displays the details.

- Check that the user name, password, and domain name are correct.
- If the **I must log on to this server** check box is selected, Websense Email Security uses simple authentication, that is, the password is passed in clear text. If you also check the **Log on using Secure Authentication** check box, the program uses secure authentication. Therefore, if you experience an invalid credentials error and you are using simple authentication, try switching to secure authentication.

Test Search for Groups and Users

The Search for Groups and Users test fails if:

- You have not specified a search base
- The search base is specified incorrectly

If the test fails, a dialog box displays the details.

- If a search base has not been specified, click the **Advanced** tab in the **Add LDAP Connection** dialog box. Click **Get Default** to get the default search base.

> **Note**
> If you connect to the server through an anonymous connection, the test may be successful without finding any groups. This is because the client has not been authenticated by the server and so does not have permission to retrieve groups.

- If you have entered a search base and the test still fails, check the search base for errors and check with the LDAP server administrator to confirm that you have specified a valid search base for the server.

Successful tests

If all 3 tests pass, a dialog box confirms the result.

Related topics

- *Configuring an LDAP connection*, page 146
- *Retrieving user information from a data source*, page 144

What objects

What objects scan email to identify them against a wide variety of characteristics that you specify. What objects include:

What object	Description	Find out more
Anti-Spam Agent	Digital Fingerprinting Tool Checks email against known spam cataloged in the Websense Anti-Spam database. Websense continually updates this database with the electronic signatures of known spam circulating on the Internet.	*Anti-Spam Agent object tools*, page 151
	Heuristics The ASA analyzes the email and assesses its characteristics in relation to known spam.	*Anti-Spam Agent object tools*, page 151
	LexiRules The ASA uses LexiRules to check the email for word combinations and patterns commonly seen in spam.	*Anti-Spam Agent object tools*, page 151
Anti-Virus Malware Scanning	Uses multiple third-party anti-virus (AV) scanners to detect viruses in email and attachments Can include the McAfee Anti-Virus Agent if a subscription to that scanner has been purchased	*Anti-Virus Malware Scanning (AVMS) object*, page 154
Data Security Suite	Uses Websense Data Security Suite to scan the contents of messages. The scan returns message disposition recommendations. This object is useful when Data Security Suite is deployed in the organization's IT infrastructure.	*Data Security Suite object*, page 159
Dictionary Threshold	Scans the email for words in 1 or more of the Websense dictionaries, or from a dictionary you have created.	*Dictionary Threshold object*, page 160
External Program PlugIn	Integrates Websense Email Security with an external executable or batch file.	*External Program PlugIn object*, page 162
File Attachment	Identifies the file type of an attachment.	*File Attachment object*, page 164
Illegal MIME Format	Detects whether the email or its attachments contain non-standard or malformed MIME content.	*Illegal MIME Format object*, page 166
Internet Threat Database	Detects URLs in email and checks those URLs against the Websense Internet Threat Database. This database contains URLs that contain material that has been categorized as adult/sexually explicit, drugs, gambling, hacking/spyware, etc.	*Internet Threat Database object*, page 167

What object	Description	Find out more
LexiMatch	Inspects the email for specified word combinations from the filter dictionaries.	*LexiMatch object*, page 168
Loop Detection	Detects looping of email between mail servers, for example loops due to Auto-forwarding rules on servers and auto-replies to delivery failure email.	*Connecting words together*, page 170
Message Size	Sets the maximum size for a whole email or the largest attachment to an email.	*Message Size object*, page 174
Number of Recipients	Checks whether an email is being sent to more recipients than you have allowed in a rule.	*Number of Recipients object*, page 175
Third-party Virus Scanning	Integrates with your anti-virus software to detect viruses in email and attachments.	*Third-party Virus Scanning object*, page 175
Virtual Image Agent	Checks if a graphic contains explicit adult graphics.	*Virtual Image Agent object*, page 179
Virtual Learning Agent	Scans email for patterns of words and phrases. You can train this object to recognize, for example, email content that is confidential and specific to your organization.	*Virtual Learning Agent object*, page 179
When	Controls the day and time that a rule is enabled.	*When object*, page 180

Anti-Spam Agent object

The Anti-Spam Agent (ASA) object is a powerful tool that:

- Checks email against a database of known spam.
- Analyzes email content to detect spam characteristics.

To include Anti-Spam Agent in a rule, see *Configuring the Anti-Spam Agent object*, page 151.

The Anti-Spam Agent is comprised of these tools:

- *Anti-Spam Agent: Digital Fingerprinting*, page 151
- *Anti-Spam Agent: Heuristics*, page 152
- *Anti-Spam Agent: LexiRules*, page 153

See also *Anti-Spam Agent object best practices*, page 153 and *Anti-Spam Agent object tools*, page 151.

Anti-Spam Agent object tools

The Anti-Spam Agent object uses the following tools. You can enable or disable any combination of these tools for use in a rule.

ASA tool	What it does
Digital Fingerprinting	Checks the digital fingerprint of an email against the Websense Anti-Spam database, which classifies spam and junk email content into categories, such as adult, chain letters, illegal material, and so on. For a full description of each category, see *Appendix A*, page 281.
Heuristics	Analyzes the email header and body, or just the header, to determine how closely the contents resemble spam. You can specify how sensitive the Heuristics tool is in evaluating email. The higher the sensitivity, the fewer spam-like traits are needed to trigger the rule. By default, the Heuristics tool scans the entire email. However, if you have a high-volume email environment, you can select to scan only the header, which results in a faster scan.
LexiRules	Analyzes the email for word combinations and patterns that are commonly seen in spam.

Configuring the Anti-Spam Agent object

To include the Anti-Spam Agent object in a rule:

1. Drag the Anti-Spam Agent object into position on the Rules palette. The **Properties for Anti-Spam Agent** dialog box displays.
2. Select the Anti-Spam tools to be enabled. To maximize ASA's capabilities, Websense recommends that you keep all tools enabled.
   - *Anti-Spam Agent: Digital Fingerprinting*, page 151
   - *Anti-Spam Agent: Heuristics*, page 152
   - *Anti-Spam Agent: LexiRules*, page 153
3. Click **OK**.

Related topics

- *Anti-Spam Agent object best practices*, page 153
- *Scheduling Anti-Spam Agent updates*, page 229

Anti-Spam Agent: Digital Fingerprinting

The Digital Fingerprinting tool checks the digital fingerprint of an email against the Anti-Spam database. The Anti-Spam database classifies spam into 17 categories. You can decide which kinds of content to allow, and which to block.

To Enable Digital Fingerprinting:

1. Drag the Anti-Spam Agent object onto the Rules palette. The **Anti-Spam Agent** dialog box displays.
2. Select the **Digital Fingerprinting** tab and select **Enable Digital Fingerprinting**.
3. Select the categories of spam to detect.
   a. You can check and uncheck individual categories.
   b. Checking **Select all** causes all categories to be selected. You can then uncheck individual categories.
   c. Unchecking **Select all** clears all category check boxes.

Related topics

- *Anti-Spam Agent object*, page 150
- *Anti-Spam Agent: Heuristics*, page 152
- *Anti-Spam Agent: LexiRules*, page 153
- *Reverse logic – Anti-Spam Agent object*, page 153
- *Anti-Spam Agent object best practices*, page 153

Anti-Spam Agent: Heuristics

The Heuristics tool analyzes the entire email, performing a series of tests that determine how closely an email resembles spam.

You can specify how sensitive the Heuristics tool is in evaluating email. The higher the sensitivity, the fewer spam-like traits an email needs in order to trigger the rule.

By default, the Heuristics tool scans the entire email. In high-volume email environments, however, it is quicker to scan only the header.

To enable Heuristics:

1. Select the **Heuristics** tab.
2. Select **Enable Heuristics**.
3. Use the slider to set the sensitivity level.
4. Select to scan the whole email or just the header.

Related topics

- *Anti-Spam Agent object*, page 150
- *Anti-Spam Agent: Digital Fingerprinting*, page 151
- *Anti-Spam Agent: LexiRules*, page 153
- *Reverse logic – Anti-Spam Agent object*, page 153
- *Anti-Spam Agent object best practices*, page 153

Anti-Spam Agent: LexiRules

The LexiRules tool performs the same tests as the Heuristics tool, but triggers the rule if the email has any spam-like traits. It is useful for detecting new spam that has not yet been added to the Anti-Spam database.

To enable LexiRules, click on the **LexiRules** tab and select **Enable LexiRules.**

Related topics

- *Anti-Spam Agent object*, page 150
- *Anti-Spam Agent: Digital Fingerprinting*, page 151
- *Anti-Spam Agent: Heuristics*, page 152
- *Reverse logic – Anti-Spam Agent object*, page 153
- *Anti-Spam Agent object best practices*, page 153

Reverse logic – Anti-Spam Agent object

If you select **Reverse logic**, the rule is triggered if none of the enabled ASA tools detect spam content in the email.

Anti-Spam Agent object best practices

The Anti-Spam Agent object detects spam in 2 ways:

- The Digital Fingerprinting tool detects email that is known to be spam because it has been seen and categorized by Websense in the ASA database.
- The Heuristics and LexiRules tools detect email that has the characteristics of spam.

The Digital Fingerprinting tool is extremely accurate at detecting known spam and returns virtually no false positives.

The Heuristics and LexiRules tools are highly effective in detecting new, unclassified spam. However, because they assess the likelihood that an email is spam, it is possible that legitimate email will trigger the rule. For example, a marketing newsletter could share some characteristics with a spam email (such as its use of HTML) and therefore trigger the rule.

Because of this difference, there are 2 default rules that use the ASA object:

- The first ASA rule enables only digital fingerprinting. If an email has the digital signature of known spam, it is isolated in the **Anti-Spam Agent–DFP** folder.
- The second ASA rule enables the Heuristics and LexiRules tools. If any of these tools detect a likely spam email it is isolated in the **Anti-Spam Agent** folder.

Separating these functions into 2 rules means that:

- Known spam is detected and isolated. You can be confident that email isolated by the Digital Fingerprint tool into the **Anti-Spam Agent DFP** folder is spam, and manage it accordingly.

- Email isolated by the Heuristics and LexiRules tools are kept in a separate folder, so that you can monitor which email is isolated and assess whether you need to change the sensitivity of the Heuristics tool.

Related topics

- *Anti-Spam Agent object*, page 150

Updating the Anti-Spam Agent object

Websense continuously updates the Anti-Spam Agent object. Websense recommends that you schedule regular updates to the ASA using the Scheduler. See *Scheduling Anti-Spam Agent updates*, page 229.

Anti-Virus Malware Scanning (AVMS) object

The Anti-Virus Malware Scanning object uses multiple supplied third-party anti-virus (AV) scanners to detect viruses in email and attachments. Websense Email Security uses multiple types of AV scanners to give a comprehensive scan of suspect files.

Websense Email Security breaks up an email into its component parts and passes them to the supplied AV scanners for analysis. The AV scanners report the results of the scan using the standard set of codes listed in *Appendix C*, page 303. Websense Email Security then deals with the email as specified in your rule set.

The AVMS object works independent of the Third-Party Virus Scanning object. You do not need an email specific version of your AV software, but you must disable any automatic file-level or directory-level scanning that your AV software performs on the Websense Email Security subdirectories.

Related topics

- *Internet Threat Database Real-Time Protection*, page 154
- *Configuring the Anti-Virus Malware Scanning object*, page 155
- *Scan Options - McAfee configuration*, page 156
- *Scan Options - configuration*, page 157
- *Notification footer*, page 158
- *Updating the Anti-Virus Malware Scanner*, page 158

Internet Threat Database Real-Time Protection

This function detects new email-borne threats as they are released to the Internet. This Anti-Virus Malware Scanning component protects your network from viruses, phishing, and malware in malicious URL links, using real-time URL categorization. To ensure immediate protection against these viruses, it is recommended that you use this feature:

- With at least 1 scanner in the Anti-Virus Malware Scanning object

- Within a rule that includes an “Isolate” Action object

Configuring the Anti-Virus Malware Scanning object

When you include the AVMS object in a rule, you need to specify:

- What kind of virus threats the AVMS will scan for
- What action the AVMS will take if it finds a virus
- Which files are exempt from AVMS scanning
- The message that users receive if a virus has been removed or cleaned from their email

To include the Anti-Virus Malware Scanning in a rule:

1. Drag the AVMS object into position on the Rules palette. The **Properties for Anti-Virus Malware Scanning** dialog box displays.
2. Select a virus scanner and click **Configure** to set the scan options. See *Scan Options - McAfee configuration*, page 156 and *Scan Options - configuration*, page 157 for details.
3. In the **Properties for Anti-Virus Malware Scanning** dialog, select the action that the AVMS will take if it finds a virus:
   - **No Action** – The AVMS takes no action, but the rule is triggered. This is the default action.
   - **Delete** – The AVMS attempts to delete the virus. If it cannot delete it, the rule is triggered.
   - **Clean Virus** – The AVMS attempts to clean the virus. If it cannot clean it, the rule is triggered.

   Note

   For the Authentium scanner, the actions **Delete** and **Clean** are the same.

4. If you have selected to delete or clean a virus, you can enter text to be used for the footer of a notification email.

   This text is used when the AVMS has successfully cleaned or deleted the virus from an infected email. You can use the variables listed in *Notification footer*, page 158, but the default message is

   ```
   Virus $V was detected in $A,
   by Websense Anti-Virus Malware Scanning.
   The infected file contents have been removed.
   ```

5. To ensure that email-borne threats are detected as they are released to the Internet, click the **Websense ITD Protection** tab, and then select the **Enable Websense ITD Protection** check box.
6. To specify which files will not be scanned, in the **Properties for Anti-Virus Malware Scanning** dialog box, click **Exclude Files**. The **Exclude Files** dialog box displays.

7. Click **Add**. The **Add Filename** dialog box displays.
8. Enter the filename of the file to be excluded from scanning and click **OK**. The file is listed in the **Exclude Files** dialog box. The AVMS will not scan any of the files listed.
9. Add more files as needed.

Related topics

- *Anti-Virus Malware Scanning (AVMS) object*, page 154
- *Internet Threat Database Real-Time Protection*, page 154
- *Scan Options - McAfee configuration*, page 156
- *Scan Options - configuration*, page 157
- *Notification footer*, page 158
- *Updating the Anti-Virus Malware Scanner*, page 158

Scan Options - McAfee configuration

You can specify what kind of virus threats the AVMS will detect when using the Anti-Virus Agent McAfee scanner. This functionality is available only when a separate Anti-Virus Agent subscription is purchased. Select 1, multiple, or all of the options.

Scanning method	What it does
Treat Errors as Infected	All errors generated when scanning email are assumed to be virus-related and treated in the same way.
Treat Encrypted Files as Infected	All encrypted files found when scanning email are assumed to be virus-related and treated in the same way.
Treat Macros as Infected	All macros found when scanning email are assumed to be virus-related and treated in the same way.
Heuristic Analysis	Heuristic Analysis means anti-virus software can recognize a virus without ever having seen that virus before. If the anti-virus software detects virus-like traits in a file, the AVMS treats that file as if it was infected with a virus.
Macro Analysis	All macros found are dissected and scanned for the presence of viruses. If the analysis of a macro within any scanned file reveals it to be infected, it is reported to the Anti-Virus Malware Scanning object.
Scan All Files for Macros	By default, the Anti-Virus Agent submits only files from the Document Files group to the Anti-Virus Malware Scanner for analysis. With this option selected, all files are scanned for macros, regardless of their file type and if a macro is found, it is reported to the Anti-Virus Malware Scanning object.

Scanning method	What it does
Malicious Applications	Malicious applications include any software that has effects unintended by or prejudicial to the user; usually where these effects are hidden. If the anti-virus software detects a malicious application, it reports it to the Anti-Virus Malware Scanning object.
Joke/Hoax Viruses	Joke or Hoax viruses do not destroy or interfere with the working of the computer system. They do, however, act as a nuisance to the user and can place a load on your email server. With this option selected, the anti-virus software scans files for the presence of joke/hoax viruses and if detected, a positive virus return code is reported back to the AVMS object.

Scan Options - configuration

You can specify what kind of virus threats the AVMS detects when using the Authentium scanner. Select 1, multiple, or all of the options.

Scanning method	Description
Treat Errors as Infected	All errors found when scanning email are assumed to be virus-related and are treated as such.
Treat Encrypted Files as Infected	All encrypted files found when scanning email are assumed to be virus-related and are treated as such.
Treat Unknown Result as Infected	If the scanning engine is not sure whether the file is infected when scanning an email, the email is assumed to be infected and is treated as such.
Treat Macros as Infected	If macros are found when scanning an email, the email is assumed to be infected and is treated as such.
Treat Damaged Files as Infected	If damaged files are found when scanning an email, the email is assumed to be infected and is treated as such.
Treat Unsupported Types as Infected	If unsupported file types are found when scanning an email (types that the Authentium scan engine cannot scan because it doesn't support them), the email is assumed to be infected and is treated as such.
Treat Jokes as Infected	If jokes are found when scanning email, the email is assumed to be infected and is treated as such.
Heuristics Normal	Heuristic Analysis means the anti-virus engine uses heuristic methods to attempt to identify a virus that has not been detected by the other techniques. If the heuristics analysis detects virus-like traits in a file, the Anti-Virus Malware Scanning object treats the file as if it is infected with a virus. This setting enables the “normal” level of heuristics.

Scanning method	Description
Heuristics AI	This setting enables the “Artificial Intelligence” level of heuristics.
Heuristics Paranoid	This setting enables the “paranoid” level of heuristics. This setting may generate false positives. It is not recommended.

Notification footer

If the AVMS deletes or cleans a virus from an email, you can add a footer to tell the recipient that this has happened.

As well as free text, you can insert the following variable codes into the footer.

Variable	What it means
$A	The name of the infected file
$B	The email subject
$D	The date that the email was processed
$F	The email filename
$N	The name of the triggered rule
$R	The email recipient’s name
$S	The email sender’s name
$T	The time of email processing
$V	The name of the virus detected by McAfee DLL anti-virus
$Z	The email size

For example, you could use the text:

```
Virus $V was detected in $A, by Websense Anti-Virus Malware
Scanning. The infected file contents have been removed.
```

This would add the following text to the infected email:

```
Virus (virus name) was detected in (file name) by Websense Anti-
Virus Malware Scanning. The infected file contents have been
removed.
```

Updating the Anti-Virus Malware Scanner

You can schedule regular updates to the Anti-Virus Malware Scanner using the Scheduler. This keeps your system safe against new viruses. If you are evaluating Websense Email Security, you can download updates for the duration of the 30-day evaluation period.

For more details, see *Scheduling Anti-Virus Malware Scanning updates*, page 230.

Data Security Suite object

In environments in which Websense Data Security Suite is deployed, the Data Security Suite object can be used to create rules that send messages to Data Security Suite for analysis against its policies and rules. Data Security Suite returns recommendations for disposition (block, encrypt, message is clean).

To use the Data Security Suite object, Data Security Suite must be deployed within the organization and Websense Email Security must be able to connect to the DSS server.

Configuring the Data Security Suite object

Before you can use the Data Security Suite object, the Data Security Suite server must be registered with Websense Email Security. In the Rules Administrator, go to the **Tools** > **Options** > **DSS Settings** tab. For details, see *Configuring the Data Security Suite connection*, page 139. If the Data Security Suite server is not registered, when you drag the Data Security Suite object onto the Rules palette a warning message states:

```
Cannot open Data Security Suite object.
```

To add the Data Security Suite object to a rule:

1. Drag the Data Security Suite object onto the Rules palette. The **Properties for Data Security Suite** dialog box displays.
2. Select the DSS recommendation that the rule will handle. For example, if Data Security Suite analyzes a message and returns “block”, the rule could be constructed to isolate the message in a special queue. The Data Security Suite recommendations include:
   - Block message
   - Encrypt message
   - Message is clean

   Note

   If the Data Security Suite policy has both the “block” *and* “encrypt” actions, only the “block” recommendation will be received by Websense Email Security. “Block” always has precedence over “encrypt”.

   As a best practice, it is best to create 2 separate rules for Data Security Suite scanning, one that handles the “block” recommendation, and one that handles “encrypt”.
3. Click **OK**.

Note that reverse logic is *not* supported for the Data Security Suite object.

Dictionary Threshold object

The Dictionary Threshold object uses a library of dictionaries to detect email content that your organization may want to avoid. These dictionaries contain words associated with different aspects of unwanted content, for example adult material, hate speech and gambling.

Websense Email Security is provided with the following dictionaries:

- Adult
- Alcohol/Tobacco/Drugs
- Arts/Entertainment
- Computing/Internet/hacking
- Compliance - Credit Cards
- Compliance - Finance
- Compliance - Medical Procedures
- Compliance - Personal Identifiers
- Confidential
- Finance
- Gambling
- Hate speech/Offensive
- Job search
- Medical/Healthcare
- Shopping
- Spam
- Spam Misspellings
- Sports
- Travel
- Violence/Weapons

Each word in these dictionaries is assigned a value that is used by the Dictionary Threshold object.

You can edit these dictionaries to add or delete words, or to change the values. You can also create new dictionaries. See *Dictionary Management*, page 215.

How the Dictionary Threshold object works

If words in an email match the entries in 1 or more dictionaries, the values of the words are added to produce a total. If this total is equal to, or greater than, the threshold specified in the Dictionary Threshold object, the rule is triggered.

Example:

1. Set a rule to trigger the Dictionary Threshold object for the Gambling dictionary at 150.

2. The Websense server receives an email that contains the words “baccarat”, “blackjack” and “slot machine”.
3. Each of these words has a value of 50. Therefore, 50 + 50 + 50 = 150, which equals the threshold.
4. The rule is triggered.

Related topics

- *Dictionary Threshold object*, page 160
- *Configuring the Dictionary Threshold object*, page 161
- *Dictionary Management*, page 215

Configuring the Dictionary Threshold object

To configure the Dictionary Threshold object you need to specify:

- The type of content you want the rule to detect
- The parts of the email to scan for dictionary content
- The dictionary score required to trigger the rule

To include the Dictionary Threshold object in a rule:

1. Drag the Dictionary Threshold object onto the Rules palette. The **Properties for Dictionary Threshold** dialog box displays.
2. Select the categories of email content you want to detect, or select **All Categories**.
3. Select the parts of the email you want to scan for dictionary content:
   - Entire Message
   - Header
   - Body
   - Attachments
4. Select the threshold that will trigger the rule.

   Default = 100

   Note

   If you have selected more than 1 dictionary, the threshold is cumulative across all of the selected dictionaries.

5. Click **OK**.

Reverse logic – Dictionary Threshold object

If you select the **Reverse logic** check box, the rule is triggered if the selected part of the email has a score equal to or lower than the threshold.

Related topics

- *Dictionary Threshold object*, page 160
- *How the Dictionary Threshold object works*, page 160
- *Dictionary Management*, page 215

External Program PlugIn object

The External Program PlugIn object integrates Websense Email Security with an external executable or batch file. You can use an external program to run a third-party command-line executable that does not require user input. You can use this executable to either check email for a condition, or to perform an action when an email meets a condition. The command must return a standard code (Return Value) for the external program to check for a condition.

Configuring the External Program Plugin object

1. Drag the **External Program PlugIn** object onto the Rules palette. The **Properties for External Program PlugIn** dialog box displays.
2. Click **Browse** and navigate to the file location of the external program to be used.
3. In the **Command Line Parameters box**, enter the command line parameters and message part operators.
   - For command line parameters – See the external program's documentation.
   - For message part operators that automatically add text from the email to form part of the external program trigger, see *Message Part Operators*, page 163.
4. You can set a return value and a logical condition that triggers the rule for that value. See *Return value conditions*, page 163.

   See the external program's documentation for details of standard codes that the program returns.
   - **Will Return TRUE** – The condition for the return value that triggers the rule.
   - **Return Value** – The return value that triggers the rule if it meets the Will Return TRUE condition.
5. Enter the **Timeout Period**. This is the time that Websense Email Security allows for the external program to complete its function. If the external program takes longer than the period specified, the rule is triggered.
6. Click **OK**.

Command Line parameters

You can enter parameters for the executable or batch file. A list of these parameters should be available in the documentation supplied with the PlugIn program.

Message Part Operators

Message part operators:

Operator	What it means
$F	The email file name.
$S	The sender's email address.
$R	The recipient's email address.
$D	The date that the email was processed.
$T	The time that the email was processed.
$B	The email subject.
$Z	The size of the email.
$N	The name of the triggered rule.
$W	Current working directory.
$V	The name of the virus detected by the Anti-Virus Agent.

Return value conditions

When you set a return value, you must specify the condition that will trigger the rule when using that value. The following table describes how the rule is triggered using the value in the dialog box ("N") and the condition.

Logical condition	The rule is triggered if...
Always	The value returned is N.
Never	The value returned is any other value than N.
Less than	The value returned is less than N.
Less than or equal to	The value returned is less than or equal to N.
Greater than	The value returned is greater than N.
Greater than or equal to	The value returned is greater than or equal to N.

Reverse logic – External Program Plugin object

The table describes the results if you select the **Reverse logic** check box for the External Program Plugin object.

Logical condition	Result
Always	The rule is triggered if the value returned is not N.
Never	The rule is triggered if the value returned is N.

Logical condition	Result
Less than	The rule is triggered if the value returned is greater than or equal to N.
Less than or equal to	The rule is triggered if the value returned is greater than N.
Greater than	The rule is triggered if the value is less than or equal to N.
Greater than or equal to	The rule is triggered if the value returned is less than N.

File Attachment object

The File Attachment object triggers a rule when it detects a selected, supported file type as an attachment to an email. Websense Email Security can also detect the original format of a file, even if the file has been renamed. You can add other file types if they are supported. See *Supported file types*, page 285.

Websense Email Security can also scan archive files, which it attempts to split into individual files. If successful, Websense Email Security compares the individual file types with the file types defined in the object. If unsuccessful, Websense Email Security applies a rule condition “If Message contains any archive files” to the file.

Note

If you configure the File Attachment object to trigger the rule when it detects document files, the rule is also triggered if it detects Web archive files (.mht).

The following archive file types can be detected, but not decompressed:

- ARJ (password protected)
- ARC (password protected)
- BZ2
- LBR
- LZH
- UUE.

Configuring the File Attachment object

To include the File Attachment object in a rule:

1. Drag the **File Attachment** object onto the Rules palette. The **Properties for File Attachment** dialog box displays.
2. You can select:
   - Groups of file types, such as image files.
   - Individual file types, such as .jpg, .mp3, and others.
   - The **Any attachment** check box.
3. Click **Add extension** to add file types to the list. See *Adding file types*, page 165.

4. **Advanced** – For archive files, you can select further processing:
   - **Trigger Archive file types only on archive files that cannot be decompressed**

     The rule is triggered if the archive file cannot be decompressed.

     If Websense Email Security detects an archive file that it can decompress, it will scan the component files and apply the enabled rule set to them.
   - **Trigger Archive file types on any archive file**

     The rule is triggered if any archive file is detected.
   - You can also specify that the rule is triggered only if all the files attached to an email are of the same type.
5. Click **OK**.

Related topics

- *Reverse logic – File Attachment object*, page 165
- *Adding file types*, page 165

Adding file types

Note

Ensure that the file type that you are adding is supported; Websense Email Security cannot detect unsupported file types if they have been renamed.

To add a file type to the list:

1. In the **Properties for File Attachment** dialog box, click **Add extension**. The **Add File Extension** dialog box displays.
2. Enter the file type. *Do not include the period* (".") in the extension.

   See *Supported file types*, page 285.
3. Click **OK**. The new file type is displayed in the list under the **File extensions** category.

   By default, the file type is not selected.

Reverse logic – File Attachment object

If you select **Reverse logic**, the rule is triggered if:

- No attachments are detected.

- More than 1 attachment is detected, but the attachments are not of the same file type.

Related topics

- *File Attachment object*, page 164
- *Compress Attachments object*, page 181
- *Strip Attachments object*, page 188

Illegal MIME Format object

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that specifies the format of email so that it can be exchanged between email systems. MIME email can contain text, images, audio, video or other application-specific data.

The Illegal MIME Format object detects email and attachments that do not pass the rigorous, internal deMIME-ing process.

Email can fail the Illegal MIME Format test for these reasons:

- The email has a non-standard format.
- An attachment is invalid.
- The email contains malicious code.

Recommendation: Implement the Illegal MIME Format object in a rule at the top of the rules list, and place any email that triggers the rule into a dedicated **Isolate** folder for analysis.

Warning

Some email that is detected and isolated by this object can contain viruses.

Configuring the Illegal MIME Format object

1. Drag the **Illegal MIME Format** object onto the Rules palette. The **Properties for Illegal MIME Format** dialog box displays.
2. Select which parts of the email to scan. You can select either or both check boxes:
   - **Detect non-standard message** – Scans only the body of an email to detect non-RFC standards compliant email.
   - **Detect invalid attachments** – Scans only attachments to detect files that have an invalid format and have failed to deMIME correctly.
3. Click **OK**.

Reverse logic - Illegal MIME Format object

If you select **Reverse logic**, the rule is triggered if:

- Detect non-standard message – Websense Email Security does not detect a non-RFC standards compliant email.
- Detect invalid attachments – Websense Email Security does not detect attachments that have an invalid format and have failed to deMIME correctly.

Internet Threat Database object

Use the Internet Threat Database object to prevent the sending of inappropriate Web links by email. This object detects email containing URLs and checks the URLs against the ThreatSeeker Internet Threat Database. This database classifies billions of Web sites into the following categories:

- Abused Drugs
- Adult/Sexually Explicit
- Alcohol and Tobacco
- Emerging Exploits
- Gambling
- Hacking
- Racism and Hate
- Tasteless
- Violence
- Weapons
- Websense Security Filtering (phishing/fraud/criminal)

Configuring the Internet Threat Database object, page 167

Configuring the Internet Threat Database object

To configure the Internet Threat Database, specify the categories to be detected.

1. Drag the Internet Threat Database object onto the Rules palette. The **Properties for Internet Threat Database** dialog box displays.
2. Select 1 or more URL categories to be detected, or click **Select all Categories**.
3. Click **OK**.

Note

If the Internet Threat Database fails to load, an error displays:

```
Failed to load Internet Threat Database
```

For more information, go to kb.websense.com and search for “Internet Threat Database failed to load at startup”.

Reverse logic – Internet Threat Database object

If you select **Reverse logic**, the rule is triggered if an email contains a URL that does not match any of the selected categories.

LexiMatch object

The LexiMatch object uses advanced Boolean searches to check for specific words or combinations of words. This means that you can trigger a rule when words are used in one context, for example, “breast enlargement”, but allow the same word to be used in a different context, for example, “breast cancer”.

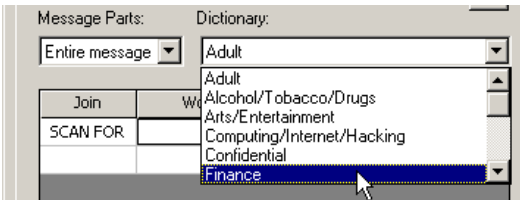
Configuring the LexiMatch object

To configure the LexiMatch object, you need to:

1. Select which parts of the email to scan for LexiMatch content.
2. Select words from the dictionaries and specify the relationship between them to create word patterns.

Including the LexiMatch object in a rule

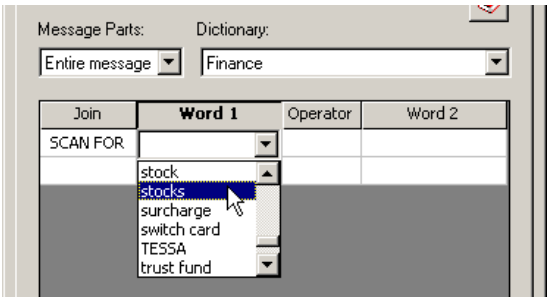
1. Drag the **LexiMatch** object onto the Rules palette. The **Properties for LexiMatch** dialog box displays.
2. Select the part of the email to be scanned for LexiMatch content:
   - Entire Message
   - Header
   - Body
   - Attachments
3. Create word patterns. Select a dictionary, for example, Finance.



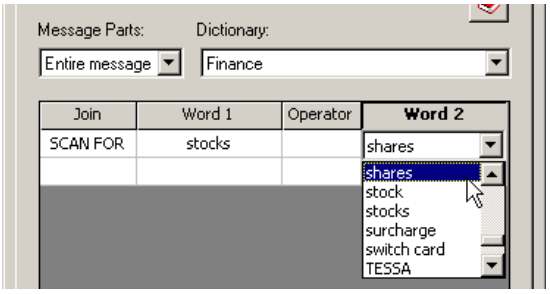
Note

You can select a different dictionary for each word in your word pattern.

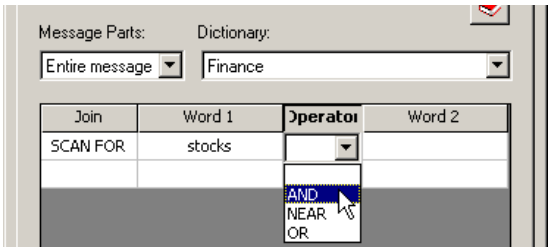
4. Select the first word in your pattern, for example, Stocks.



5. Select the second word in your word pattern, for example, Shares.



6. Select the **Operator** to define the relationship between the 2 words, for example, Stocks AND Shares. See *Connecting words together*, page 170.



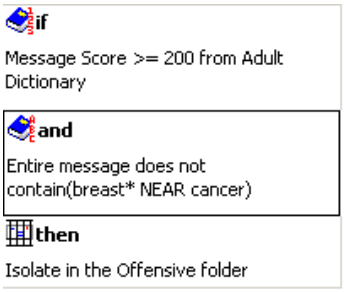
7. If your word pattern uses the NEAR operator, you can change the NEAR distance. This is the number of characters between the first letter of the first word and the first letter of the second word. See *Using the NEAR word operator*, page 170.
8. You can join word patterns together with the JOIN operator. See *Joining word patterns together*, page 171.
9. Click **OK**.

Reverse logic – LexiMatch object

If you select **Reverse logic**, the rule is triggered if the email does not contain the specified words or word patterns, or the word patterns do not meet the specified conditions, for example, NEAR distance.

Reversing the logic of a LexiMatch object is useful if you combine the LexiMatch object with a Dictionary Threshold object. For example, you can create a rule that is triggered if it detects words from the “Adult” dictionary, which would not trigger if the same words were used in, for example, a medical context.

This rule shows the reverse logic LexiMatch object with a Dictionary Threshold object.



Connecting words together

There are 3 operators you can use to join words from the dictionary.

Operator	Example word pattern	What it does
AND	Red AND Blue	If the scanned part of the email contains the word **Red** and the word **Blue**, the rule triggers. The words can occur any distance apart and in any order.
OR	Red OR Blue	If the scanned part of the email contains either the word **Red** or the word **Blue**, the rule triggers.
NEAR	Red NEAR Blue	If the scanned part of the email contains both **Red** and **Blue** within the number of characters specified in the NEAR distance, the rule triggers. If the 2 words are further apart than the specified NEAR distance, the rule does not trigger.

Using the NEAR word operator

When you create a word pattern using the NEAR operator, Websense Email Security uses the distance between the first letter of the first word and the first letter of the second word as the NEAR distance.

You can set a different NEAR distance in each rule that uses the LexiMatch object.

Joining word patterns together

You can also join word patterns together to form more sophisticated combinations by using JOIN commands.

Command	Example	What it does
AND	Phrase A AND Phrase B	The rule is triggered if the scanned part of the email contains Phrase A and Phrase B.
AND NOT	Phrase A AND NOT Phrase B	The rule is triggered if the scanned part of the email contains Phrase A but NOT Phrase B.
OR	Phrase A OR Phrase B	The rule is triggered if the scanned part of the email contains either Phrase A or Phrase B.
OR NOT	Phrase A OR NOT Phrase B	The rule is triggered if either: • The scanned part of the email contains Phrase A. • The scanned part of the email does not contain Phrase A and also does not contain Phrase B.

Loop Detection object

The Loop Detection object detects email that loops on single or multiple email servers. The Loop Detection object marks each email passing through it with a unique domain ID. If the mark is already there, the Loop Detection object recognizes that it has been processed before and checks it for looping.

The best way to deal with looping email is to isolate it in a dedicated folder.

Configuring the Loop Detection object, page 171

Configuring Delivery Failure loop detection, page 173

Advanced settings, page 173

Reverse logic – Loop Detection object, page 174

Configuring the Loop Detection object

To include the Loop Detection object in a rule you need to specify:

- How many occurrences of an email will trigger the rule.
- The condition that will identify the email as looping:
  - Greater than or equals – if the occurrences of 1 email reach the number specified in Message Occurrences, or higher, the loop detection object will trigger.
  - Equals – if the occurrences of 1 email reach exactly the number specified in Message Occurrences, the loop detection object will trigger.

The Loop Detection object also checks the header to detect delivery failure notices. Because looping is commonly caused by delivery failure notices, you can set the Loop Detection object to trigger the rule when it encounters the email header of a delivery failure notice. By default, the loop detection object will trigger the rule if the header contains any of the following:

- <>
- could not be sent
- delivery failure
- postmaster
- report-type=delivery status.

You can edit this list – see *Configuring Delivery Failure loop detection*, page 173.

However, email that contains a non-delivery item in the header needs to loop only once to be isolated. This is independent of the number of occurrences you set.

Also, email that contains a non-delivery item in the header and also the same address for both sender and recipient is isolated the first time it is detected. However, if anti-spoofing (see *Anti-Spoofing*, page 41) is enabled, the email is isolated by the anti-spoofing function.

To include the Loop Detection object in a rule:

1. Drag the Loop Detection object onto the **Rules** palette. The **Properties for Loop Detection** dialog box displays.
2. **Message occurrences** – Enter the number of occurrences of the same email that will trigger the rule.

   Default = 5
3. Enter the condition that will trigger the rule:
   - Greater than or equals

     The rule is triggered if the number of times that the email passes through Websense Email Security is greater than or equal to the **Message occurrences** setting.
   - Equals

     If the number of times that the email passes through Websense Email Security is equal to the **Message occurrences** setting.
4. Click **OK**.

Related topics
- *Loop Detection object*, page 171
- *Configuring Delivery Failure loop detection*, page 173
- *Advanced settings*, page 173
- *Reverse logic – Loop Detection object*, page 174

Configuring Delivery Failure loop detection

1. In the **Delivery Failure loop detection** area, click **Configure**. The **Delivery Failure Configuration** dialog box displays.
2. Click **Add**. The **Add message header text** dialog box displays.
3. Enter the text to be used to identify delivery failure messages, for example "Failure Notice". The Loop Detection object checks the message header for this text string.
4. Click **OK**.

The text string displays in the **Delivery Failure Configuration** dialog box.

Related topics

- *Loop Detection object*, page 171
- *Configuring the Loop Detection object*, page 171
- *Advanced settings*, page 173
- *Reverse logic – Loop Detection object*, page 174

Advanced settings

You can configure the following advanced settings:

- **Unique Identifier** – The Loop Detection object uses a unique identifier to track email as it passes through Websense Email Security. The default number that is generated during installation is displayed in the box, but you can edit this number. If you are running Websense Email Security on more than 1 server, you should edit the number to ensure that all servers in your domain share the same Unique Identifier.
- **Forwarded Messages** – Looping is sometimes caused by auto-forwarding email as attachments. You can specify the number of levels of nesting that are allowed in forwarded email before triggering the loop detection object.

  Default = 3

  Maximum level of nesting = 25

To configure the advanced settings:

1. In the **Properties for Loop Detection** dialog box, click **Advanced**. The **Advanced** dialog box displays.
2. **Unique Identifier** – Enter the code to be used as a unique identifier for email.

   Maximum = 36 characters
3. **Forwarded Messages** – Enter the number of levels of nesting to allow in forwarded email.

   Default = 3

Maximum = 25

Related topics
- *Loop Detection object*, page 171
- *Configuring the Loop Detection object*, page 171
- *Configuring Delivery Failure loop detection*, page 173
- *Reverse logic – Loop Detection object*, page 174

Reverse logic – Loop Detection object

The table describes the results of selecting **Reverse logic** for the Loop Detection object.

Condition	Result
Greater than or Equals	The rule is triggered if the email passes through Websense Email Security less than N times.
Equals	The rule is triggered if the email does not pass through Websense Email Security exactly N times.

Related topics
- *Loop Detection object*, page 171
- *Configuring the Loop Detection object*, page 171
- *Configuring Delivery Failure loop detection*, page 173
- *Advanced settings*, page 173

Message Size object

The Message Size object enables you to restrict the size (in KB) of email or files sent as attachments to email.

Configuring the Message Size object

1. Drag the Message Size object onto the Rules palette. The **Properties for Message Size** dialog box displays.
2. Enter a value for the maximum size of either:
   - The total size of an email
   - The size of the largest file attachment in an email
3. Click **OK**.

Reverse logic – Message Size object

If you select **Reverse logic**, the rule is triggered if an email or attachment is smaller than the maximum size specified.

Number of Recipients object

The Number of Recipients object limits the number of recipients that can receive a given message. This can be useful for managing bandwidth.

Configuring the Number of Recipients object

To include the Number of Recipients object in a rule:

1. Drag the **Number of Recipients** object onto the Rules palette. The **Properties for Number of Recipients** dialog box displays.
2. Enter the maximum number of recipients for any single message. The rule is triggered if an email has more than this number of recipients.
3. Click **OK**.

Reverse logic – Number of Recipients object

If you select **Reverse logic**, the rule is triggered if an email is sent to fewer than the maximum number of recipients specified.

Third-party Virus Scanning object

The Third-party Virus Scanning object uses your third-party anti-virus (AV) scanning software to detect viruses in email and attachments. Websense Email Security can use multiple types of AV scanners to give a comprehensive scan of suspect files.

Websense Email Security breaks an email into its component parts and passes them to the AV scanners for analysis. The AV scanners report the results of the scan using the standardized set of codes listed in *Appendix C*, page 303. Websense Email Security then deals with the email as specified in your rule set.

The Third-party Virus Scanning object works independent of the Anti-Virus Malware Scanning object. You do not need an email specific version of your AV software, but you must disable any automatic file level or directory-level scanning that your AV software performs, at least on the Websense Email Security subdirectories.

For a list of supported scanner types, see *Integrated Third-Party Virus Scanners*, page 176.

To configure a third-party virus scanner, see:

Configuring the Third-Party Virus Scanning object, page 176

Configuring a command line scanner, page 177

Configuring a SAVSE scanner, page 177

See also:

Reverse logic – Third-Party Virus Scanning object, page 177

Multiple Virus scans, page 178

Avoiding conflicts with Third-Party anti-virus products, page 178

Integrated Third-Party Virus Scanners

Websense Email Security is fully integrated with the AV scanners listed below. Alternatively, you can configure the Third-Party Virus Scanning object to use any command line-based AV product.

Type	Scanner	Find out more
DLL based	Sophos SAVI	*Configuring the Third-Party Virus Scanning object*, page 176
Command line	McAfee/Network Associates NetShield Executable (scan.exe)	*Configuring a command line scanner*, page 177
ICAP	Symantec Anti-Virus Scan Engine (SAVSE)	*Configuring a SAVSE scanner*, page 177

Recommended: For sites with high volumes of email traffic, Websense recommends using DLL based scanners. DLL scanners are usually faster because they reside in computer memory.

Configuring the Third-Party Virus Scanning object

1. Drag the Third-Party Virus Scanning object onto the Rules palette. The **Properties for Third-Party Virus Scanning** dialog box displays.
2. Click **Add**. The **Select Virus Scanner** dialog box displays. DLL-based scanners are marked as such.
3. Select a scanner from the list and click **OK**.

   See the following procedures to configure each type of scanner:

   - DLL – No procedure, the scanner displays in the **Selected Third-Party Virus Scanners** list.
   - Command line – *Configuring a command line scanner*, page 177.
   - If your scanner is not in the list, click **Other Vendor**.
   - ICAP – *Configuring a SAVSE scanner*, page 177.
4. After you have selected and configured the scanner, select the scan evaluation code that will trigger the rule.

   If your scanner returns a value equal to or higher than this code, the Anti-Virus Scanning object triggers the rule.

   For example, if you set the code to 001 and the anti-virus scanning software reports with code 010, it means that either:

   - A virus has been found
   - There was an error scanning the file
5. Click **OK**.

Reverse logic – Third-Party Virus Scanning object

If you select **Reverse logic**, the rule is triggered if the third-party virus scanner returns a scan evaluation code less than the specified scan evaluation code.

Configuring a command line scanner

1. Drag the Third-Party Virus Scanning object onto the Rules palette. The **Third-Party Virus Scanning object** dialog box displays.
2. Click **Add**. The **Select Virus Scanner** dialog displays.
3. Select the command line scanner to be used. If your AV product is not in the list, click **Other Vendor**.
4. Click **OK**. The **Anti-Virus Product Configuration** dialog displays.
5. In the **Anti-Virus Executable** box, enter or browse to the location of the **.exe** file for your scanner. If you selected an integrated anti-virus product, the default location is displayed automatically. See *Integrated Third-Party Virus Scanners*, page 176.
6. The **Default Parameters** entry field contains the command line instructions for your anti-virus scanner. The default parameters are displayed automatically for integrated scanners.

   Codes for third-party virus scanners that are not integrated are listed in the documentation supplied with your virus scanning software.
7. Enter a value in the **Timeout Period** field. This is the amount of time that Websense Email Security will wait for a scan to complete. If the virus software does not respond within this time, Websense Email Security moves on to the next processing step in the rule.
8. Click **OK**.

The scanner is displayed in the Properties for Third-Party Virus Scanning dialog box.

Configuring a SAVSE scanner

To include the Third-Party Virus Scanning object in a rule using Symantec SAVSE:

1. Drag the Third-Party Virus Scanning object onto the Rules palette. The **Anti-Virus Scanning Object** dialog box displays.
2. Click **Add**. The **Select Virus Scanner** dialog box displays.
3. Select **Symantec Anti-Virus Scan Engine (SAVSE)**.
4. Click **OK**. The **Third-Party Virus Product Configuration** dialog box displays.
5. Click **Add**. The **SAVSE Server Configuration** dialog box displays.
6. In the **SAVSE Server IP** text box enter the IP address of the SAVSE Server.

   If SAVSE is installed on the same machine as Websense Email Security, enter 127.0.0.1.
7. Click **Test**. If the connection is successful, a message shows the virus definition date.

If Websense Email Security cannot connect to the SAVSE server, an error message is displayed. Check that the IP address is correct.

8. In the **SAVSE Server Port Number** text box enter the port that Websense Email Security will use to communicate with the SAVSE server.
9. In the **Fail Retry Time** text box enter the length in seconds that Websense Email Security will wait before retrying a connection if the first connection is unsuccessful.
10. In the **Scan Timeout** text box enter the amount of time that Websense Email Security will wait for the scan to complete. If the virus software does not respond within this time, Websense Email Security moves on to the next processing step in the rule.
11. Click **OK**. The SAVSE scanner is listed in the **Anti-Virus Product Configuration** dialog box.
12. Click **OK**. The SAVSE scanner is listed on the **Properties for Third-Party Virus Scanning** dialog box.
13. Select the virus code that will trigger the rule. If your selected anti-virus scanner returns a value equal to or higher than this code, the Third-Party Virus Scanning object triggers the rule.

    For example, if you set the Scan Evaluation Code to 001 and the virus scanning software reports with code 006, this means that either:

    - A virus has been found
    - There was an error scanning the file
14. Click OK.

Multiple Virus scans

You can allow multiple virus scans of the same file when:

- You have enabled more than 1 rule that uses the Third-Party Virus Scanning object.
- You have configured the Third-Party Virus Scanning object to use more than 1 third-party virus product.

By default, after an email has been scanned once, the results of the scan are carried over and applied when there is a further instance of the Third-Party Virus Scanning object. To re-scan the email each time, select the **Force Scan** check box on the Third-Party Virus Scanning object dialog box.

Avoiding conflicts with Third-Party anti-virus products

Occasionally there can be a conflict when third-party anti-virus software is installed on the Websense server, and the Websense Email Security Rules Service and the anti-virus service try to access the **\In** folder simultaneously. This can occur whether or not the Anti-Virus Agent or Websense Third-Party Virus Scanning object are part of a rule.

To prevent this conflict:

- Exclude the Websense root directory from real-time scanning.
- Do not use your anti-virus software to scan inbound files. You can continue the real-time scanning of outbound email.

Virtual Image Agent object

The Virtual Image Agent (VIA) is a powerful image recognition tool that scans graphics files for explicit adult content.

You can set the sensitivity of the analysis. Although a higher sensitivity will detect a higher number of explicit adult images, there will also be a higher number of false detections.

The VIA is an optional component that requires a separate subscription. If you are an evaluating customer, you can use the VIA object for the duration of your 30-day evaluation period.

Configuring the VIA object, page 179

Configuring the VIA object

To include the VIA object in a rule:

1. Drag the Virtual Image Agent object onto the Rules palette. The **Properties for Virtual Image Agent** dialog box displays.
2. Set the sensitivity.
3. Click **OK**.

Reverse logic – VIA object

If you select **Reverse logic**, the rule is triggered if an email contains images and none of them are flagged by VIA using the specified settings.

Virtual Learning Agent object

The Virtual Learning Agent (VLA) scans email for patterns of words and phrases. It uniquely valuable because you can train it to detect email that contains words or phrases that you have identified as company-confidential or business-critical. This protects your organization from security risks that can arise from leaked information.

Note

Before you can use the VLA object in a rule, you must train the VLA to recognize the content that you want to detect. See *Virtual Learning Agent*, page 253.

Configuring the VLA object

To include the VLA object in a rule:

1. Drag the Virtual Learning Agent object onto the Rules palette. The **Properties for Virtual Learning Agent** dialog box displays.
2. Select the VLA category that you want to detect.

Reverse logic – VLA object

If you select **Reverse logic**, the rule is triggered if an email does not contain any content that the VLA object recognizes as belonging to a trained VLA category.

When object

Use the When object to control the day and time that a rule is active. For example, you can combine a When object with a Message Size object so that large files are only allowed to be sent over your network outside working hours, when demand for bandwidth is lower.

Configuring the When object

To set the time when a rule is active you can specify:

- The time of day that the rule will start and finish
- The days of the week that the rule is active
- A calendar period when the rule is active

To include a When object in a rule:

1. Drag the When object onto the Rules palette. The **Properties for When** dialog box displays.

   Note
   The rule is triggered if email is detected within the time period that you set.

2. In the **Start** and **Finish** boxes, enter the times that the rule is to start and finish. The When object uses the 24-hour clock. For example:

   Start 09:00:00

   Finish 17:00:00
3. Enter either:
   - The days of the week that the rule will be active, such as Monday - Friday.
   - The calendar day that the rule will start and/or finish. For example:

     Trigger after 19 January 2008

     Trigger before 25 January 2008

     This means the rule will be active between January 19 and 25, 2008.
4. Click **OK**.

Reverse logic – When object

If you select **Reverse logic**, the rule is triggered if the time is outside the start and finish times and days or dates that you have set.

Operations objects

Operations objects make changes to either an email or parts of an email, such as the header.

Operations object	What it does
Compress Attachments object, page 181	Compresses attachments into a single archive, reducing the size of the email.
Footers and Banners object, page 182	Adds a footer or a banner to the email.
Header Modification object, page 184	Edits, removes or appends email header fields.
HTML Stripper object, page 185	Removes active HTML content from the email.
Routing object, page 186	Redirects email to the mail server or MTA you specify.
Save Copy object, page 187	Stores a copy of the email in a specified location.
Strip Attachments object, page 188	Removes attachments from email before sending to the recipient.
TLS Delivery object, page 189	Forces the message to be sent encrypted.

Compress Attachments object

Use the Compress Attachments object to compress file attachments. This reduces email file size and conserves network bandwidth.

To configure, see *Configuring the Compress Attachments object*.

For details of supported file types, see *Supported file types*, page 285.

You can also:

- Select to create a log entry of this operation in the system database.
- Specify a name of the file that will contain the compressed attachments.

Configuring the Compress Attachments object

To include the Compress Attachments object in a rule:

1. Drag the **Compress Attachments** object onto the Rules palette. The **Properties for Compress Attachments** dialog box displays.
2. Select the file types you want Websense Email Security to compress:

- All attachments
- Attachments of the type selected. Go to step 3.
- Attachments of the type not selected. Go to step 4.

You can add supported file types to the list. See *Adding file types*, page 182.

3. If you selected **Attachments of the type selected**, select the file types to compress. You can select groups of file types, such as audio files, or individual file types, such as .mp3 files.
4. If you selected **Attachments of the type not selected,** select those file types that are *not* to be compressed.
5. To specify logging and file options, click **Advanced properties**. The **Advanced Properties** dialog box displays.
   a. To record that an attachment has been compressed, select **Log this operation to the database**.
   b. If needed, specify the name of the file that will contain the compressed attachments.

      Default = attachments.zip
   c. Click **OK** to return to the **Compress Attachments** dialog box.
6. Click **OK** to accept the changes.

Adding file types

If you have added a file type when configuring the File Attachment object (see *File Attachment object*, page 164), the file type will already be included in the **Compress Attachments** list.

For details of supported file types, see *Supported file types*, page 285.

To add a file type to the list:

1. When you have clicked **Add extension** in the **Properties for Compress Attachments** dialog box, the **Add File Extension** dialog box displays.

   Enter the file type, but do not include the period (“.”) character in the extension.
2. Click **OK**. The new file type is displayed in the list under the **File extensions** category.

   By default, the file type is not selected.

Footers and Banners object

You can add footers and banners to an email, for example to act as a disclaimer. A footer is attached at the end of an email, a banner at the beginning.

When you use the Footers and Banners object in a rule, you need to decide:

- To add either a footer or a banner.
- If the footer or banner is to be included in all email, or for selected users or groups.

- The text of the footer or banner.
- If the footer or banner will override the previous one.

Configuring the Footers and Banners object

1. Drag the **Footers and Banners** object onto the Rules palette. The **Properties for Footers and Banners** dialog box displays.
2. Specify who the footer and banner applies to. This can be:
   - A domain

     For example: mycompany.com
   - An individual user

     For example username@mycompany.com
   - Leave the box blank to apply the footer to all users
3. You can:
   - Type the footer text, and include variables (see *Footer and Banner variables*, page 183).
   - Import text from a text file (see step 6).
4. By default, a footer is added. To add banner text, select **Add text as Banner**.
5. If you have several footer objects in your rules, but want only 1 to be displayed on any individual email, select **Override previous footer or banner**. This adds only the last footer of your rules logic to an email.
6. To import Footer and Banner text from a text file, click **Import** and select your text file from the **Import Footer** dialog box. Click **Open**. The text is displayed in the **Text** area.

   Footer and banner sample text is provided in:

   \Websense Email Security\SampleFooter.txt

Footer and Banner variables

The table lists the variables you can use in footer or banner text.

Variable	Description
$B	The email subject.
$C	The dictionary score.
$D	The date that the email was processed.
$F	The email filename.
$N	The name of the triggered rule.
$R	The email recipient’s name.
$S	The email sender’s name.
$T	The time of email processing.

Variable	Description
$V	The name of the virus detected by the Anti-Virus Agent.
$Z	The size of the email.

Header Modification object

You can use the Header Modification object to change email header field values, such as the Subject, return path or To fields.

A common use is to apply it to a generic incoming email account, such as customerservices@mycompany.com, to replace the To field with the email address of the responsible individual in the organization.

To include the Header Modification object in a rule you need to decide:

- Which field of the email is to be changed.
- What changes you want to make to that field.
- Whether there are any exceptions or whether Websense Email Security will always change the field.

Header modification – actions, page 185

Header modification – fields, page 185

Configuring the Header Modification object

To include the header modification object in a rule:

1. Drag the **Header Modification** object onto the Rules palette. The **Properties for Header Modification** dialog box displays.
2. Click **Add**. The **Edit Header Field Modification** dialog box displays.
3. From the **Action** drop-down list, select an action. This is the change you want to make in the header field.
   - Find/Replace
   - Remove
   - Add/Overwrite
   - Add/Append
   - Add/Prepend

   See *Header modification – actions*, page 185/
4. In the **Field name** drop-down list, select the field to be changed. See *Header modification – fields*, page 185.
5. Enter the field parameters. The fields that are available depend on the action you selected.

   A summary of your selected action is displayed. For example:

   Find “customerservice@mycompany.com” in the “To:/Cc” field and replace with “andy@mycompany.com; maewong@mycompany.com”

6. Click **OK**.

Header modification – actions

The table describes the actions you can perform on header fields. Not all actions are available for every header field. For example, you cannot perform a remove operation on email path fields (X-Envelope-To, To/Cc, From or Return Path).

Action	What it does
Find/Replace	Finds specific text in the header field and replaces it with your text.
Remove	Removes the field. This has different results for different fields: • If you remove the Subject field, only the subject description is removed and not the field itself. For example, an email with Subject: Hello would read Subject:. • If you remove the Received and Message ID fields, both the fields and the contents are removed.
Add/ Overwrite	Overwrites all the contents of the field with your text.
Add/Append	Adds your text after the contents of the field.
Add/Prepend	Adds your text before the contents of the field.

Header modification – fields

Email fields you can modify:

Field	Description
X-Envelope-To	The delivery information of the email.
To/Cc	The email addresses on the To: or Cc: list.
From	The sender's identity.
Return-Path	The address that a reply to the email is sent to.
Reply-To	The originator of the email.
Subject	The text in the Subject line of an email.
Received	The date and time the email was received.
Message-ID	The email identifier.
Return-Receipt-To	The address to which receipts are sent.
Disposition-Notification-To	The address to which disposition notifications are sent.

HTML Stripper object

Use the HTML Stripper object to remove HTML content and/or active HTML components from the body of email. Active content is code that can execute on a client PC (such as JavaScript, VBScript, Java applets or ActiveX objects), often

without the user's permission. Active content can also include malicious actions executed by the mail client when the user is viewing the email.

Configuring the HTML Stripper object

1. Drag the **HTML Stripper** object onto the Rules palette. The **Properties for HTML Stripper** dialog box displays.
2. Select how Websense Email Security will remove HTML content if the rule is triggered:
   - **Remove active HTML components**

     Select the types of HTML content to remove, such as:
     - Scripts: JavaScript, VBScript etc.
     - IFrame: independent HTML frames
     - Active links
     - ActiveX and software objects
     - Java applets
   - **Remove the HTML from multi-part email and deliver the text-only email body**

     Multipart and alternative email contains both a plain text and an HTML part. Which part is shown to the recipient is determined by its email client, and (in some cases) by its choice. The HTML Stripper object can remove the HTML from this kind of email so that the recipient can view only the email in its plain text form. Non-multipart alternative HTML email is delivered with no email body.

     You can select to either:
     - Remove all active HTML components
     - Remove the HTML content entirely. This may result in an empty email body.
3. Click **OK**.

Routing object

The Routing object can redirect email that triggers rules to the mail server or MTA of your choice. For example, if your organization has an archiving policy, the Websense Email Security can send a copy of email that meets your archiving criteria to the archiving server, while processing the original email as normal.

Note

Before you can use the Routing object in rules, you need to configure Smart Host Routing in the Server Configuration console. See *Smart Host routing*, page 82.

Configuring the Routing object

1. Drag the Routing object onto the Rules palette. The **Properties for Routing** dialog box displays.

2. Select what to redirect:
   - Each message that triggers a rule.

     Websense Email Security continues to process the email and then redirects it to the server that you specify, unless further rules are triggered that lead to the email being isolated or discarded.
   - A copy of each mail that triggers the rule.

     Websense Email Security immediately sends a copy of the email to the server that you specify, without processing it further. The original email is processed as normal.
3. If a copy is redirected, you need to choose the state of the email.
   - Current message state

     Websense Email Security redirects a copy of the email in the condition it is in at the current stage of processing. For example, if the email has had its HTML content stripped by a preceding rule, the email is redirected without its HTML content.
   - Original message state

     Websense Email Security redirects the email exactly as it was when it was placed in the **In** folder. For example, if the email has had its HTML content stripped by a previous rule, the email is delivered with its HTML content still present.
4. Select the server that you want to redirect the email to. The Smart Host server list displays any Smart Hosts you have configured. To configure a Smart Host see *Smart Host routing*, page 82.
5. Click **OK**.

Save Copy object

Use the Save Copy object to save a copy of a sent or received email to a folder that you specify.

When you install Websense Email Security, the setup program creates a folder at a default location that you can use to save a copy of messages. However, you can specify a different location when you configure the object to use in a rule. You can also select whether the email is to be saved in its current (after processing) or original (before processing) form.

Configuring the Save Copy object

1. Drag the Save Copy object onto the Rules palette. The **Properties for Save Copy** dialog box displays.
2. Enter or browse to the folder where you want to save email.
3. Select how you want email to be saved:

   Copy original message – Example: If the email has had its HTML content stripped by a previous rule, a copy of the email is saved with its HTML content intact.

Copy current message state – Example: If the email has had its HTML content stripped by a preceding rule, a copy of the email is saved without its HTML content.

4. Click **OK**.

Strip Attachments object

Note

If an archive file (for example, a .zip file) contains a file type that triggers a rule containing the Strip Attachments object, the archive file is stripped from the email.

The Strip Attachments object removes attachments from email before allowing it to proceed to its destination. You can remove all attachments or just specific formats.

For a list of supported file types, see *Supported file types*, page 285.

Configuring the Strip Attachments object

1. Drag the Strip Attachments object onto the Rules palette. The **Properties for Strip Attachments** dialog box displays.
2. You can select:
   - Groups of file types, such as image files
   - Individual file types, such as .jpg, .mp3, and so on
   - The **Remove all message attachments** check box
3. To add an extension to the list, click **Add extension**. For details see *Adding file types*, page 188.

Adding file types

If you have added a file type when configuring the File Attachment object (see *File Attachment object*, page 164), the file type is already included in the Strip Attachments list.

To add a file type to the list:

1. In the **Properties for File Attachment** dialog box, click **Add extension**. The **Add File Extension** dialog box displays.
2. Enter the file type. *Do not* include the period (“.”) character in the extension.
3. Click **OK**. The new file type is displayed in the list under the **File extensions** category.

By default, the file type is not selected.

TLS Delivery object

Include the TLS Delivery object in a rule when you want to require that a matching message be sent encrypted, regardless of server configuration settings.

> **Warning**
> Messages marked “TLS Delivery” that are routed through connections that do not support TLS will not be delivered.

Configuring the TLS Delivery object

1. Drag the TLS Delivery object onto the Rules palette. The **Properties for TLS Delivery** dialog box displays.
2. Click **OK**.

Notify objects

The Notify objects allow you to send an email notification to a user when a rule has been triggered. The table lists the Notify objects.

Notify object	What it does
Blind Copy object, page 189	Copies an email that has triggered a rule to an interested third party, such as the systems administrator.
Email Notification object, page 191	Notifies an interested party that a rule has been triggered, including the details of the rule.

Blind Copy object

The Blind Copy object sends a blind copy of the email that has triggered a rule to the user you specify.

When you use the Blind Copy object, you need to know:

- Who you want to blind copy the email to. For example, you might want to blind copy the email to your organization’s HR manager.
- Whether you want to replace the subject text.

  You can replace the subject text of the email so that the user knows that they are receiving a blind copy notification before they open the email. For example, if you were notifying the HR department that a rule had been triggered, you could change the subject line to “This email breaches the AUP”.
- Whether you want the blind copy recipient to be able to reply directly to the email sender, or to the systems administrator.

Configuring the Blind Copy object

Use the Blind Copy object to send a blind copy of the email that has triggered a rule to a specific user.

To configure the Blind Copy object:

1. Drag the Blind Copy object onto the Rules palette. The **Properties for Blind Copy** dialog box displays.
2. Specify who should receive the blind copy:
   - **Domain Administrator** – Select the check box.
   - To blind copy another user, enter their email address in the **Add new bcc recipient** field, and click **Add**. The address is displayed in the email address area.
3. To remove an email address, select it in the list and click **Remove**.
4. To replace the subject text, select **Replace Subject Text** and enter the new text in the field. See below for a list of variables you can use in the field.
5. For replies to the blind copy email to be delivered to the Domain Administrator, select **Return Path to Domain Administrator**.
6. Click **OK**.

Subject text variables:

Variable	Description
$B	The email subject.
$C	The dictionary score.
$D	The date that the email was processed.
$F	The email filename.
$N	The name of the triggered rule.
$R	The email recipient's name.
$S	The email sender's name.
$T	The time of email processing.
$V	The name of the virus detected by the Anti-Virus Agent.
$Z	The email size.

Example:

"This email has triggered $N and was sent by $S"

In the Subject line, the variable substitutions identify the triggered rule and the name of the email sender.

Email Notification object

Use the Email Notification object to inform users that a rule has been triggered. For example, you can notify the sender, the recipient, the system administrator, and an HR representative.

Warning
Do not attach an email that you suspect is infected with a virus.

Before including the Email Notification object in a rule, you need to know:

- Who will be notified. For example, the email sender and their line manager.
- What the notification email will say. In addition to your open text, you can include the several variables in the subject line and body.

  Email notification object variables, page 193
- Whether you want to include the email that triggered the rule in the notification email. There are 2 ways to do this:
  - Attach the original message.
  - Attach the current message state.

Configuring the Email Notification object

To include the Email Notification object in a rule:

1. Drag the Email Notification object onto the Rules palette. The **Properties for Email Notification** dialog box displays.
2. Specify who the email is from. You can:
   - Select a standard option:

     Domain Administrator – If the rule is triggered by an email from a protected domain, this is the email address that you set in the Protected Domain Properties dialog box in Server Configuration (see *Adding Protected Domains*, page 40).

     If the rule is triggered by an email that is not from a protected domain, this is the email address that you set in the Administration dialog box in Server Configuration (see *Administration settings - general*, page 86).

     In the email notification, the “From” and “Return Path” fields contain this address.

     Empty Return Path – In the email notification, the “From” field contains the Domain Administrator address, the “Return Path” field is empty.
   - Enter any email address. For example: test@mail.com.

     In the email notification, the “From” and “Return Path” fields contain this address.
3. Specify who to send the email notification to. You can:
   - Enter 1 or more recipients in the **To** text box. Separate multiple addresses by semicolons.

- Select 1 or more of the standard options:
  - **Message Sender**
  - **Domain Administrator** – If the rule is triggered by an email from a protected domain, this is the email address that you set in the Protected Domain Properties dialog box in Server Configuration (see *Adding Protected Domains*, page 40).

    If the rule is triggered by an email that is not from a protected domain, this is the email address that you set in the Administration dialog box in Server Configuration (see *Administration settings - general*, page 86).
  - **Message Recipients**

4. Enter the subject of the email.

   Default = **Autonotify $B**.

   Edit the subject line using text or variables. See *Email notification object variables*, page 193.

5. To attach the email that triggered the rule, select **Include Message as Attachment**, and then select 1 option:
   - **Attach original message** – Example: If the email has had its HTML content stripped by a previous rule, a copy of the email will be saved with its HTML content still present.
   - **Attach current message state** – Example: If the email has had its HTML content stripped by a preceding rule, a copy of the email will be saved without its HTML content.
6. Click **OK**.

Email notification object variables

Variable	Description
$A	The names of any attachments that have been stripped from the email.
$B	The email subject.
$C	The dictionary score.
$D	The date that the email was processed.
$F	The email filename.
$N	The name of the triggered rule.
$R	The email recipient's name.
$S	The email sender's name.
$T	The time of email processing.
$V	The name of the virus detected by the Anti-Virus Agent.
$Y	Inserts the first 10KB of the body of the email.
$Z	The email size.

Related topics

- *Protected Domains*, page 39
- *Administration settings - general*, page 86

Actions objects

The Actions objects determine what action to take if an email meets the conditions of the rule. If an email triggers a rule that contains an Action object, no more rules are applied to that email. The email is moved to the **Out** folder ready for delivery into the recipient's mailbox.

Without Actions objects, email messages pass through Websense Email Security to their destination, even if they trigger a rule.

The Actions objects include:

Allow object	What it does	Find out more
Allow Message	Places the email in the **Out** folder for delivery.	*Allow Message object*, page 194
Delay Message	Delays the delivery of the email until the time you specify.	*Delay Message object*, page 194

Allow object	What it does	Find out more
Discard Message	Irrevocably deletes the email	*Discard Message object*, page 195
Isolate Message	Places the email in the folder you specify so that you can review and analyze it.	*Isolate Message object*, page 195

Allow Message object

Use the Allow Message object for positive filtering. For example, you could allow all email from your CEO to pass through Websense Email Security with the minimum of rules checking, but check email from other members of your organization more thoroughly.

Configuring the Allow Message object:

1. Drag the Allow Message object onto the Rules palette. The **Properties for Allow Message** dialog box displays.
2. Select **Log this Action to Rules Database** to create an entry in the logging database when a email is allowed.
3. Click **OK**.

Delay Message object

Use the Delay Message object to delay the sending or receipt of messages that are likely to place undue load on your network. For example, you could delay email over a certain size until non-working hours.

When you use a Delay Message object in a rule, email that triggers the rule is held in the **Delay** folder until the time you specify. To specify the time that delayed email is released, you need to configure the Delay Queue in the Server Configuration console. See *Queue management*, page 68.

Configuring the Delay Message object

To include a Delay Message object in a rule:

1. Drag the Delay Message object onto the Rules palette. The **Properties for Delay Message** dialog box displays.
2. Click **OK**.

Discard Message object

Use the Discard Message object to delete email, for example, email with attachments that are found to be virus infected. If an email triggers a rule that contains a Discard Message object, the email is deleted and no further rules are applied to it.

Warning

You cannot retrieve email that has been discarded.

You can select to log Discard Message activity to the Websense Email Security database. However, if your 30-day evaluation period expires, email activity logging stops.

Configuring the Discard Message object

To include the Discard Message object in a rule:

1. Drag the Discard Message object onto the Rules palette. The **Properties for Discard Message** dialog box displays.
2. To create an entry in the logging database when an email is discarded, select **Log this Action to Rules Database**.
3. Click **OK**.

Isolate Message object

The Isolate Message object places email that has triggered a rule into a separate folder where you can review and analyze them. Once an email has been isolated, no further rules are applied to it.

When you include the Isolate Message object in a rule, you specify which of the available queues store the email that triggers that rule.

Websense Email Security comes with these preconfigured queues:

- Anti-Spam Agent - DFP
- Anti-Spam Agent
- Compliance
- Confidential
- Delay
- Dictionaries - Spam
- File Formats
- Internet Threat DB - Inappropriate
- Internet Threat DB - Spam
- Isolate
- Network Security
- Offensive
- Virtual Image Agent
- Virus
- VLA - Spam

To add other queues, see *Adding a queue*, page 69.

> **Note**
> If you are upgrading Websense Email Security from a previous version, new queues are *not* created.

Configuring the Isolate Message object

1. Drag the Isolate Message object onto the Rules palette. The **Properties for Isolate Message** dialog box displays.
2. Select the folder (for example **Isolate**) to be used to isolated email that has triggered the rule.
3. Click **OK**.

8 Message Administrator

The Message Administrator allows you to review, manage, and analyze email that has been placed in queues, and to view a record of Websense Email Security activity. You can:

- Configure the Message Administrator
- Manage email
- Analyze email

Message Administrator components include:

The Queues toolbar, page 208

Message Search panel, page 201

Queues panel, page 202

Logs panel, page 203

Message List panel, page 203

Message Parts panel, page 206

Message Contents panel, page 207

See also *Working with queues*, page 207.

Opening the Message Administrator

To open the Message Administrator select

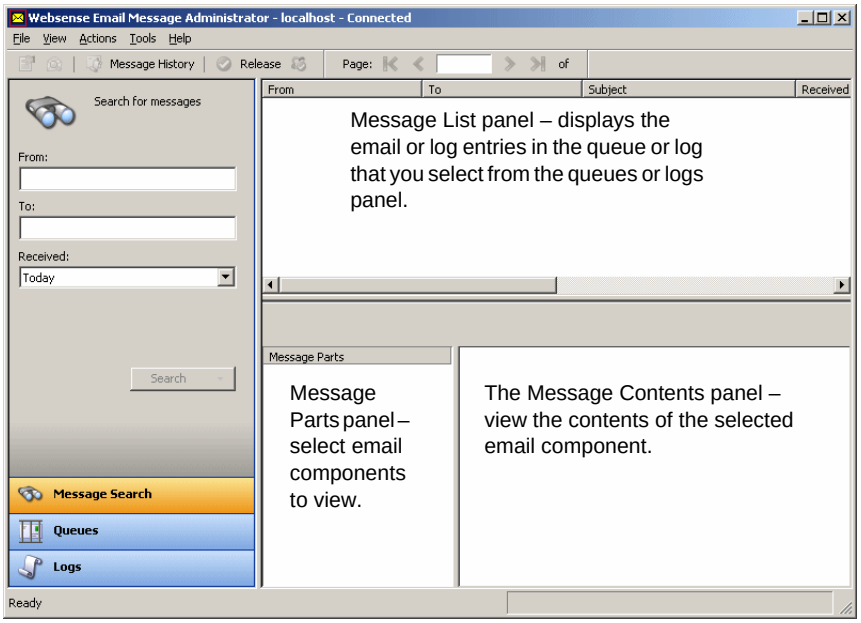
Start > Programs (or **All Programs**) **> Websense Email Security > Message Administrator**

The Message Administrator window displays.

The Message Administrator window

The Message Administrator window:

Message Search panel – search for email in the database.



Queues and Logs panels – select a queue or log to display their contents.

Configuring Message Administrator

Configure the Message Administrator with the **Options** dialog box.

- *Opening Message Administrator Options*, page 198
- *General tab*, page 198
- *Messages tab*, page 199
- *File Types tab*, page 200
- *HTML Viewer tab*, page 200
- *Columns tab*, page 200

Opening Message Administrator Options

To open the Message Administrator options select **Tools** > **Options**.

The **Options** dialog box displays.

General tab

Use the **General** tab to:

- Specify the file that Websense Email Security uses to automatically reply to email. For example, to tell an email sender that their email has not been delivered.

- Specify whether files are automatically saved and where to save them.

Setting	Description
Auto-Reply File	The location of the auto-reply text file used to generate responses to specific types of email. The default is Autoreply.txt in your Websense Email Security root directory. You can edit this file or create a new one using a text editor. See *Appendix D*, page 305 for more information.
Automatically save files when selected	Select this check box to automatically save files to the identified directory when you click **Save**. If this check box is not selected, Websense Email Security always prompts you to confirm the save operation.
Folder to save files	Select the directory where you want to automatically save files.

Messages tab

The **Messages** tab controls:

- The number of messages displayed in the Message List panel for the Message Search and the queues and log records.
- How Websense Email Security behaves when you perform an action on an email.

You can set the number of pages to display, and the number of items to display on each page for the Message Search function, the queues and the log records. Examples:

- If Websense Email Security is running on the same machine as the Message Administrator, or you have a fast connection, use the default settings.
- If you have a slow connection, for example, over a dial-up modem, it is recommended that you reduce the number of messages and log records displayed.

Message Administrator - default settings

Display	Items per page	Number of pages
Message Search	50	10
Queues	50	200
Logs	50	200

The **Messages** tab also contains the following options:

- **Confirm when deleting message** – Select this to be prompted to confirm deletion of the selected email.
- **Confirm when releasing all messages** – Select this to be prompted to confirm release of messages from the selected queue when you click either **Release** or **Release All**.
- **Notify when new messages arrive** – Select this to display a notification pop-up when a new email arrives at the Message Administrator.

- **Select the following message part by default** – Select the message part from the drop-down list. This is the part of an email that is displayed when you click the email in Message Administrator.

File Types tab

The **File Types** tab controls which file types you can open through the Message Administrator.

You can view only HTML files within the Message Administrator. To view any other type of file, you need an external viewer installed on your computer. You will be prompted to open non-HTML files using an external viewer. Click **Always Open** or **Never Open** to avoid being prompted.

> **Note**
> Message Administrator does not control which viewer is used to view files. The viewer is determined by your Windows File Associations.

For each file type, you can select one of the following options:

- **Always Prompt** – Select this option for the Message Administrator to display a prompt that asks if you want to display the file content for each instance of the file type.
- **Always Open** – Select this option for the Message Administrator to automatically display the file contents of the file type in the associated viewer.
- **Never Open** – Select this option for the Message Administrator to never open files of the selected type.

HTML Viewer tab

The **HTML Viewer** tab gives you the option of viewing the active HTML content of messages while you are reviewing them in the Message Contents panel. This can represent a security risk, as active HTML content can contain malicious code.

Websense recommends that all the check boxes remain cleared and that you avoid viewing active HTML content if possible.

Columns tab

Use the Columns tab to specify which columns are visible when you are viewing queues and logs.

From the **Change the columns for** drop-down, select which set of columns is to be changed. The visible columns are shown in the **Visible Columns** list.

Moving columns

To move a column:

1. Select the column in the **Visible Columns** list.
2. Click the arrows to move the column up or down in the list.

Inserting columns

To insert a column:

1. Click **Insert**. The **Choose a Column** dialog box displays.
2. Select the column to insert and click **OK**.

Hiding Columns

To hide a column:

1. Select the column in the **Visible Columns** list.
2. Click **Hide**.

When you have made your changes, click **Apply** and click **OK**. The **Options** dialog box closes and you return to the Message Administrator.

Using Message Administrator

This section describes the panels in the Message Administrator:

- *Message Search panel*, page 201
- *Queues panel*, page 202
- *Logs panel*, page 203
- *Message List panel*, page 203
- *Message Parts panel*, page 206
- *Message Contents panel*, page 207

Message Search panel

When you open Message Administrator, the Message Search panel is the default view. You can search for inbound and outbound email within supplied, selectable date ranges, or your own custom date range.

The **Received** list refers to the date that Websense Email Security received the email.

You can select to search using friendly names and email addresses, or using only email addresses, which is faster. To select this, click the down arrow part of the Search button.

Example

Robert sent an email to a number of people and Simon says he has not received it. Robert contacts you to find out what happened. You use Message Search to search for recent email from Robert to Simon.

All matches are shown in the Message List panel. The search names or part names can be anywhere in the sender's or receiver's friendly name or email address. By default, the results are shown in reverse chronological order.

You select the likely email and its details are displayed in the Message Parts panel and the Message Contents panel. However, these views are only available for messages that are in the queues.

Related Topic
- *Message History*, page 202

Message History

You can further examine details of the email by clicking **Message History** on the toolbar.

The details in this view could, for example, tell you that the recipient's email gateway was unavailable.

If you want to send these details to other interested parties, you can save in the following formats:

- Complete Web page (*.htm, *.html)
- Web archive (*.mht)
- HTML-only Web page (*.htm, *.html)
- Text file (*.txt)

Queues panel

The Queues panel shows:

- The Delay and Isolate queues
- Any other queues that you have configured using Server Configuration. See *Queue management*, page 68.

You can display the contents of a queue for:

- Today
- Yesterday
- Last 7 days
- Last 30 days
- All records

To the right of each queue is the number of records that it currently contains. Click a queue or log to display its contents in the Message List panel.

Logs panel

For the period you select, this panel shows a list of:

- Connection log – The connections from the host servers to Websense Email Security.
- Receive log – Email that has been received by Receive Service.
- Rules log – Email that has triggered a rule, including the rule name, policy type and the size of the email.
- Audit log – Actions that have been carried out on messages, including the audit user, audit type and activity for each email.
- Send log – Email that has been received and released by the Send Service, including the route, IP address of the mail server, size of the email and the SMTP code.
- System log – All system activity.

You can display the contents of a queue for periods of:

- Today
- Yesterday
- Last 7 days
- Last 30 days
- All records

To the right of each queue is the number of records that it currently contains. Click a log to display its contents in the Message List panel.

Message List panel

The Message List panel shows all messages in a selected queue or log.

A typical example of email in the System Log:

Arranging columns

You can show, hide, move or resize columns to show only the information that you need.

Showing or Hiding Columns

To hide a column, right-click the column heading and select **Hide**. The column is removed from the Message List panel.

To show the column, right-click any column heading, select **Insert** and select the column from the list.

Moving Columns

To move a column, click the column heading and drag the column into position. A blue line indicates where the column will be dropped when you release the mouse button.

Resizing Columns

To change the width of a column, drag the line between columns.

Sorting

You can sort your list of email on any of the column headings displayed. Click the column heading once to sort in ascending order; click the column again to sort in descending order.

Sorting a column generates a new search and adds it to the query list. You can then save the query by selecting **Save Query** from the View menu. The next time you open the queue, you can select the query from the list and the results will be sorted again.

You can combine sorting with queries to create a powerful searching tool.

This query shows messages isolated on the same day, ordered alphabetically by subject.

Date	Subject	File Name	Rule Name	Recipients
19/08/2006 02:00:12		014_1750ino143.pro		not.real.add@n...
19/08/2006 02:00:12		012_41ino7e3.pro		not.real.add@n...
19/08/2006 02:00:11	FW: *Enterprise Support Weekly Newsletter for 00...	014_1144inoed42.pro		not.real.add@n...
19/08/2006 02:00:10	Get to Know Yourself -- and Your Friends!	118_0047ino1c8b.pro		not.real.add@n...
19/08/2006 02:00:11	Get to Know Yourself -- and Your Friends!	018_0047ino1c8b.pro		not.real.add@n...
19/08/2006 02:00:12	hey buddy	012_41ino76e.pro		not.real.add@n...
19/08/2006 02:00:11	My new email address	018_0103ino1ccc.pro		not.real.add@n...
19/08/2006 02:00:11	My new email address	118_0103ino1ccc.pro		not.real.add@n...
19/08/2006 02:00:11	nowhere.com | $5 off Summer's Not Over sale goe...	118_0058ino1cbd.pro		not.real.add@n...
19/08/2006 02:00:11	nowhere.com | $5 off Summer's Not Over sale goe...	018_0058ino1cbd.pro		not.real.add@n...
19/08/2006 02:00:11	RE:	014_1529inod2.pro		not.real.add@n...
19/08/2006 02:00:12	RE:	012_41ino97e.pro		not.real.add@n...
19/08/2006 02:00:12	RE: FW: Roll-up Quote and specs	014_1148inoed45.pro		not.real.add@n...

Listing isolated email by subject is a good way to keep track of spam because spammers change their address regularly.

To learn more about searching, see *Searching for email using menu functions*, page 205.

Quick search - shortcut menu

You can use the shortcut menu to search quickly for email with the same criteria, such as a specific date, rule name, subject, and so on. The text in the shortcut menu corresponds to the heading in the table.

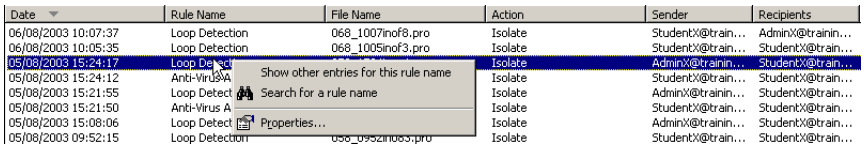
Example: If you select the Rule Name column for an email, the first option in the shortcut list is “Show other entries for this rule name”.

Example: If you select the Sender column for an email, the first option in the shortcut list is “Show other entries for this sender”.

To use the shortcut menu:

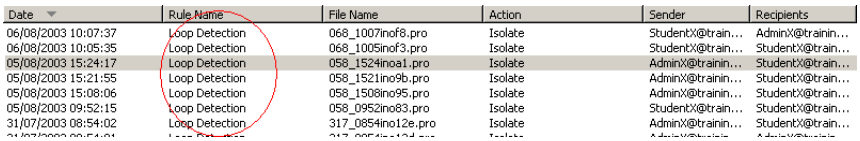
1. Right-click the column for an email.

The example uses the Loop Detection rule.



2. Select the first option “Show other entries for this rule name”.

   The table is sorted to display only entries that have triggered the Loop Detection rule.



3. Further search the sorted list using other criteria, such as recipients, subject, date, and so on.

   Example: Search for email that triggered the Adult rule, and then search that email for a specific sender’s email address.

Related Topic

- *Message List panel*, page 203

Searching for email using menu functions

In addition to the Message Search function (see *Message Search panel*, page 201), you can use the menu functions to search for email.

To search queues and logs for email:

1. Select **View** > **Find**. The **Find** dialog box displays.
2. From the **Search field** drop-down list, select the field to be searched. You can search any of the fields within the Message Administrator.
3. In the **Find what** text box, enter the words to search for.
4. Select the **Match whole word only** check box to find just the results that exactly match the text you entered. Otherwise, the search finds text strings that contain the word you have entered. For example, a search for “hotmail.com” will match on “gareth@hotmail.com”, “Susie@hotmail.com”, “dave@hotmail.com”, and so on.
5. Click **Find** to start your search.
6. To save your search criteria, select **View** > **Save Query**. When you exit Message Administrator, unsaved search criteria is cleared.
7. Enter a name for the query in the **Query name** field in the **Search** dialog box. If you do not name the query, Websense Email Security automatically assigns a name.
8. To use your search again, select it from the drop-down list.

Saved queries are displayed in blue text in the query list; unsaved queries in black. Unsaved queries are lost if you select a different queue or log, or if you close Message Administrator.

9. To return to the previous query, click  .

Related topics

- *Quick search - shortcut menu*, page 204
- *Message Search panel*, page 201
- *Message List panel*, page 203

Message Parts panel

Note

The Message Parts panel is displayed only if you are viewing email stored in a queue. If you are viewing a log, the Message Parts panel is not available.

The Message Parts panel breaks out the following parts of the email:

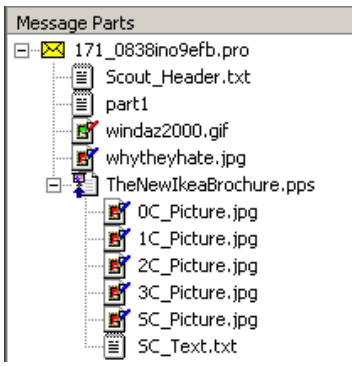
- The email header
- The body
- Attachments

In the panel, click the part of the email to be displayed.

The Message Administrator uses its internal viewer to display the part in the Message Contents panel. If the Message Administrator cannot display the selected component in its internal viewer, it gives you the option of viewing the component in an external viewer for that file type.

Viewing decomposed email

When the Document Decomposition object is fully enabled, Text, Pictures and OLE Embedded objects are extracted from the compound files. A decomposed file is then represented as a container, holding its decomposed data.



Related topics

- *Configuring Document Decomposition*, page 136

Message Contents panel

Note

If Document Decomposition is enabled, HTML in the body of an email or in an attachment is decomposed into 2 files: sc_text.txt containing the visible text, and sc_URLS.txt containing any URLs. See *Configuring Document Decomposition*, page 136.

The Message Contents panel displays the contents of the part of the email that you have selected in the Message Parts panel. If available, you can also display attachments.

Related topics

- *Message Parts panel*, page 206

Working with queues

When you are viewing a queue in the Message List panel, you can:

- View the details of an email – *Viewing email properties*, page 208
- Forward a copy of an email – *Forwarding a copy of the selected email*, page 210
- Reply to the sender of an email – *Replying to the sender of an email*, page 210
- Submit an email to the Anti-Spam Agent database – *Submitting an email to the Anti-Spam Agent database*, page 211
- Analyze an email to understand why it triggered dictionary rules – *Analyzing email*, page 209
- Release individual or multiple email – *Releasing email*, page 211
- Move email to a different queue – *Moving email*, page 211
- Save a copy of an email – *Saving copies of email*, page 211
- Delete email – *Deleting email*, page 211
- Delete all email from a queue – *Deleting all email from a queue*, page 212
- Work with queues on multiple servers – *Working with queues on multiple servers*, page 212
- Work with logs – *Working with logs*, page 212

- Use queues and logs with multiple servers – *Working with queues on multiple servers*, page 212

The Queues toolbar

The Queues toolbar is only available when viewing the contents of email in the Message List panel. Some buttons are available for single selections only.

Queues toolbar buttons:


Show information about the selected email, including details of recipients and file size. Single selections only.


Analyze the contents of the selected email using one or more of the Websense dictionaries. Single selections only.


Forward a copy of the selected email to any email address. This does not delete the email. Single selections only.


Reply to the email sender. Single selections only.


Submit the selected email to Websense for inclusion in the Anti-Spam Agent database. Single selections only.


Release the selected email for delivery.


Move the selected email from the current folder to an alternative folder. For example, move email from the Delay queue to the Isolate queue.


Save the selected email.


Delete the selected email.


Delete all email from the selected queue.

Viewing email properties

You can display detailed information about an email, including the name of the rule triggered by the email, the time and date that the Websense Email Security engine processed the rule, and the Dictionary score for the email if it triggered a Dictionary Threshold rule.

To view the details of an email:

1. Select the email from the list.
2. Click  . Detailed information displays in the **Properties** dialog box.

3. Click **Analyze** to perform a detailed dictionary analysis on the email. See *Analyzing email*, page 209 for details.
4. Click **OK**.

Analyzing email

When you analyze an email, you can view each word that has triggered the dictionary rule, how often it occurs and its score.

To analyze an email:

1. Select the email from the list.
2. Click  . The **Analyze File** dialog box displays.
3. You can filter the results further by selecting from the drop-down lists:
   - Dictionary
   - Message Part
   - Scoring
4. Select the dictionary that you want to use to analyze the email.

   The list displays statistics for:
   - The words from the email that appear in the selected dictionary
   - The part of the email in which the words occur
   - The value assigned to each word
   - The number of these words found
   - The individual word scores
   - The total word score
5. From the **Message Part** drop-down list, you can select which parts of the email to scan:
   - The entire email
   - The email header
   - The email body
   - The email attachments
6. From the **Scanning** drop-down list, select either:

   Threshold Total – Displays the dictionary scoring words from the highest scoring part of a multi-part alternative email with more than one Message Body. Depending on which part of an email is the highest scoring part for the selected dictionary determines which part of the email is displayed.

   Grand Total – Displays the dictionary scoring words from all selected parts of an email. In the case of a multi-part alternative email with more than one Message Body, identical dictionary scoring words from alternative parts will have a cumulative effect on the final score for the selected dictionary.
7. Click **OK** to return to Message Administrator.

Forwarding a copy of the selected email

You can forward an email from a queue. For example, you might want to forward a copy of an email that has been isolated for inappropriate content to the sender's manager or the HR department. The email is forwarded as an attachment.

To forward a copy of an email:

1. Select the email in the list.
2. Click  . The **Forward** dialog box displays.
3. In the **To** field, enter the email addresses that you want the email forwarded to.
4. Specify who you want to receive copies of the email. Select any or all of the following:
   - Message Sender
   - Message Recipients
   - Systems Administrator
5. By default, the subject of the forwarded email is displayed in the **Subject** text field, but you can change it.
6. You can type a message in the **Body** text field. For example, "This email has been isolated because it contains material that could be deemed inappropriate".
7. Click **Send**. The email is sent with annotation that identifies it as being from your Mail Administrator's mailbox. The original email remains in its current queue.

Replying to the sender of an email

To reply to the sender of an email:

1. Select the email in the list.
2. Click  . The **Reply to Sender** dialog box displays.
3. To send a copy of the reply to another person, enter their email address in the **BCC** field.
4. To send a copy of the reply to the Systems Administrator, select the **BCC Admin** check box.
5. For the email, you can either:
   - Select from a range of standard auto-reply messages in the **Auto-Reply message format** drop-down list.
   - Select **Clear** from the **Auto-Reply message format** drop-down list and enter your own message in the text box.
6. Click **Send**.

The email is sent with annotation that identifies it as being from the Mail Administrator's mailbox. The original email remains in its current queue.

Submitting an email to the Anti-Spam Agent database

To submit an email to the Anti-Spam Agent database:

1. Select the email in the list.
2. Click  . The **Submit to Anti-Spam Agent** dialog box displays.
3. The address and subject are entered automatically by Websense Email Security. You can change the **Subject** field.
4. Click **OK**.

The email is sent to Websense, Inc. where it is assessed for addition to the Anti-Spam Agent categories. The original email remains in its current queue.

Releasing email

To release email:

1. Select one or more messages in the list.
2. Click  . The email is moved to the **Send** queue.

If you have selected the option **Confirm** when releasing all messages in the Message Administrator options, a confirmation pop-up displays.

Moving email

To move email:

1. Select one or more messages in the list.
2. Click  . The **Move to Queue** dialog box displays.
3. Select the queue to move the email into.

You can also drag an email into a queue in the Queues panel.

Saving copies of email

To save a copy of 1 or more messages:

1. Select the email in the list, or the individual email part in the Message Parts panel.
2. Click  to open the **Save As** dialog box.
3. Select the file name and location for the email and click **Save**.

Deleting email

To delete an email select the email in the list and click  .

If you have selected the option **Confirm when deleting messages** in the Message Administrator options, a confirmation message is displayed.

Deleting all email from a queue

To delete all email from a queue select the queue in the Queues panel and click  .

If you have selected the **Confirm when deleting messages** in the Message Administrator options, a confirmation message is displayed.

Working with queues on multiple servers

If you have Websense Email Security installed on more than one server and they are sharing a SQL database, the features of Message Administrator are available from any server. For example, an email in the Isolate folder on Server A can be released using Message Administrator on Server B. However, you cannot use Message Administrator to move email from one server to another.

To use Message Administrator on multiple servers, Websense Email Security must be configured as follows:

- All Websense Email Security servers must share the same domain.
- The Administration Server services on each machine must be logged on using a domain account with network privileges. An account on the local machine, or within a workgroup, is not sufficient.
- If the server is logging to a remote SQL Server using Windows Authentication, all the services need to be logged on using this Domain account, and the account must have sufficient database access privileges as well. (You can use SQL Authentication for this).

For more information about configuration options, see the *Websense Email Security Installation Guide*.

Working with logs

You can view the following logs:

- **Connection log** – The connections from the host servers to Websense Email Security.
- **Receive log** – Messages that have been received by Receive Service.
- **Rules log** – Messages that have triggered a rule, including the rule name, policy type and the size of the email.
- **Audit log** – Actions that have been carried out on messages, including the audit user, audit type and activity for each email.

- **Send log** – Messages that have been received and released by the Send Service, including the route, IP address of the mail server, size of the email and the SMTP code.
- **System log** – All system activity.

To display the properties of an individual log record, double-click the record in the Message List panel.

Using queues and logs with multiple servers

If you are using more than one Receive Service, for example, in a large organization with more than one mail server, it is possible that 2 different .msg files could be given the same name. To distinguish between servers, you can display the server name for each email.

To display the server name in the queue or log:

1. Select any log.
2. In the **Message List** panel, right-click any column heading.
3. Select **Insert**. The **Choose a Column** dialog box displays.
4. Select **Server Name** and click **OK**.

A Server Name column is included on the email list panel that displays the name of the server that each email belongs to.

9 Dictionary Management

Dictionaries are used by such tools as the *Dictionary Threshold object*, page 160 and the *LexiMatch object*, page 168.

By adding dictionaries and by adding words to the provided dictionaries, you can optimize dictionary filtering results.

Opening Dictionary Management

To open Dictionary Management select

Start > Programs (or **All Programs**) **> Websense Email Security > Dictionary Management**

The Dictionary Management window displays.

See *The Dictionary Management window*, page 215.

The Dictionary Management window

The Dictionary Management window lists all of the dictionaries available to Websense Email Security. The provided dictionaries are listed under **Websense Dictionaries**. Added dictionaries are listed under **Custom Dictionaries**.

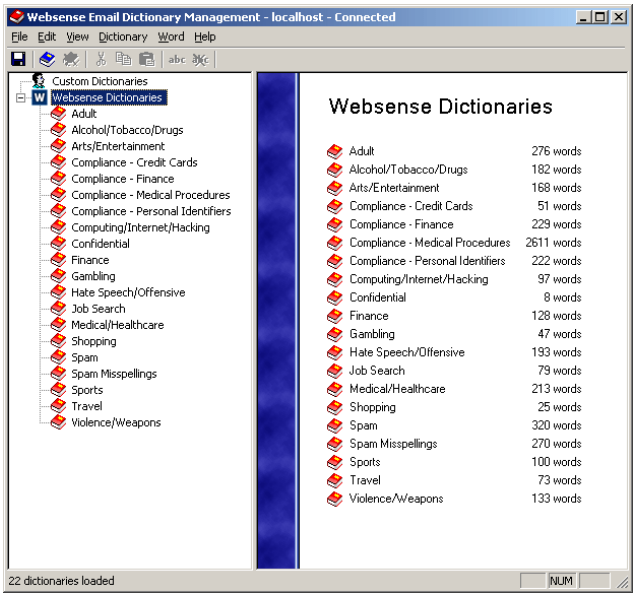
Click on a dictionary to display the words it contains and their scores.

The Dictionary Management window.

If you add a dictionary, it is displayed under Custom Dictionaries.

The provided dictionaries are listed here.

Click a dictionary to display the words it contains and their scores.



Navigation Panel

Display Panel

Initially, the number of words in the dictionaries are displayed.
When you click a dictionary in the left panel, the words that it contains and their scores are displayed in the right panel.

Related topics

- *Dictionary Management toolbar*, page 216
- *Adding a dictionary*, page 217
- *Adding words or phrases to a dictionary*, page 217
- *Importing dictionaries*, page 222

Dictionary Management toolbar


Save the changes you made to the dictionaries.


Create a new dictionary.


Delete a dictionary.


Cut selected words to paste into another dictionary.


Copy selected words onto the clipboard to paste into another dictionary.


Paste words from the clipboard into a dictionary.

Add a word to the selected dictionary.


Delete a word from the selected dictionary.

Adding a dictionary

To add a dictionary:

1. Open the **Dictionary Management** window.
2. Click New Dictionary  . The **Add/Edit Dictionary** dialog box displays.
3. Enter a name and a description for the dictionary.
4. If you want to display a warning message when the dictionary is opened, for example if the dictionary contains offensive words, enter a message in the **Warning Message** field and select **Display this message when dictionary launches**.
5. Click **OK**.

   The new dictionary displays under Custom Dictionaries.

   You can now select the dictionary when using the dictionary-based rules objects, for example, the LexiMatch object.
6. Click  to save your changes.

Related topics

- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220
- *Deleting words from a dictionary*, page 220
- *Deleting a dictionary*, page 221
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Adding words or phrases to a dictionary

Note

To use the Confidential dictionary in rules, you need to add the words and phrases that signify confidential content in your organization.

You can add words or phrases to a dictionary and give them a score. You can also use number pattern recognition, wildcards and binary sequences to make dictionary scanning tools more powerful. See:

Using number pattern recognition, page 218

Using wildcards, page 219

Using binary sequences, page 219

To add words or phrases to a dictionary:

1. Open **Dictionary Management**.
2. Click on the dictionary to which you want to add words. The list of existing words and scores displays in the right panel.
3. Click  . The **Add/Edit Phrase** dialog box displays.
4. Enter the word or phrase to be included in the dictionary.
5. Enter a value between 0 and 100 for the word or phrase.

   The higher the score, the fewer instances of the word or phrase need to appear in an email to trigger a Dictionary Threshold rule.
6. Click **OK.** The new word or phrase is added to the list of words in the dictionary.
7. Click  to save your changes.

Related topics

- *Adding a dictionary*, page 217
- *Editing dictionary words*, page 220
- *Deleting words from a dictionary*, page 220
- *Deleting a dictionary*, page 221
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Using number pattern recognition

You can add any pattern of numbers to a dictionary using the # character to signify a single number.

For example #### #### #### #### will find the credit card number 1234 5678 9011 1213, but not the string abcd 1234 defg 5678.

Using number pattern recognition can prevent email users from transmitting potentially sensitive data, such as credit card details, account numbers or patient file numbers.

Related topics

- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220

Using wildcards

You can use wildcards to make the Websense Email Security dictionary scanner more extensive. With no wildcards, a word is assumed complete and separated by white space or punctuation marks. With wildcards, you can scan parts of words.

> **Note**
> You cannot place one wildcard character immediately next to another.

You can use the following wildcard characters.

Wildcard	Description and example
*	One or more characters at the beginning or end of a word or phrase. Example: sex* finds sexy or sexily, but not Essex.
?	A single character in a word or phrase. Example: jo?n would match john and joan, but not johann.
^	One or more white-space characters.
!	A single white-space or punctuation character.
\	An escape character.

Related topics

- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220

Using binary sequences

You can also search for binary sequences. Use this ability to identify specific binary file sequences expressed as hexadecimal sequences.

To enter a binary sequence, enter `~ followed by an even number of hexadecimal characters that represent the search sequence.

For example `**~61626364** is the Binary representation of abcd.

A rule to detect this binary sequence will trigger if an email contains the following strings:

- abcd
- abcdxxxabcdxxx

The phrase **ABCD** will not trigger the rule because the binary code distinguishes between upper and lower case letters.

Related topics

- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220

Editing dictionary words

To change a dictionary word or its score:

1. Open **Dictionary Management**.
2. Click the dictionary to edit. The list of words in the dictionary and their scores displays in the right panel.
3. Double-click a word or score, and change the details.
4. Click  to save your changes.

Related topics

- *Adding a dictionary*, page 217
- *Adding words or phrases to a dictionary*, page 217
- *Deleting words from a dictionary*, page 220
- *Deleting a dictionary*, page 221
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Deleting words from a dictionary

If you delete words used by objects in an enabled rule, the rule becomes ineffective and email containing those words simply passes to the next processing step.

To delete words from a dictionary:

1. Open **Dictionary Management**.
2. Select a dictionary. The dictionary word list and scores displays.
3. Select one or more words to delete. Select multiple words using Shift or Ctrl.
4. Click  . The selected words are removed from the dictionary.
5. Click  to save your changes.

Related topics

- *Adding a dictionary*, page 217
- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220
- *Deleting a dictionary*, page 221
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Deleting a dictionary

You can delete any of the dictionaries. If you delete a dictionary, rules that use threshold scores from that dictionary or LexiMatch object become ineffective and email continuing words from that dictionary pass to the next processing step.

If you delete a dictionary by mistake, you can restore it by importing the Websense dictionary pack. See *Importing a Websense Email Security dictionary pack*, page 222.

To delete a dictionary:

1. Open **Dictionary Management**.
2. Click the dictionary to be deleted. The list of words in the dictionary and their scores displays in the right panel.
3. Click  . A confirmation message displays.
4. Click **Yes** to delete the dictionary, or **Cancel** to cancel the action.
5. Click  to save your changes.

Related topics

- *Adding a dictionary*, page 217
- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220
- *Deleting words from a dictionary*, page 220
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Importing dictionaries

There are 2 ways to import a dictionary into Websense Email Security:

- *Importing a Websense Email Security dictionary pack*, page 222
- *Importing a unicode text file*, page 223

  Import a Unicode text file to create a new dictionary or to overwrite the contents of an existing dictionary.

Related topics

- *Adding a dictionary*, page 217
- *Adding words or phrases to a dictionary*, page 217
- *Editing dictionary words*, page 220
- *Deleting words from a dictionary*, page 220
- *Deleting a dictionary*, page 221
- *Exporting dictionaries*, page 224

Importing a Websense Email Security dictionary pack

By default, Websense Email Security installs the English language dictionaries. You can add other language dictionaries using the Import-Export utility.

Dictionaries are provided for the following languages:

- Dutch
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish
- Traditional Chinese
- Simplified Chinese

To import a Websense Email Security dictionary pack:

1. Open **Dictionary Management** and select **File > Import/Export dictionary pack**. The **Import/Export Utility** wizard opens.
2. Click **Next**. The **Select Source and Target** dialog box displays.
3. Select **Import from file**.
4. Enter or browse to the location of the dictionary file.

By default, the Websense dictionaries are in the folder:
Websense Email Security\Language Packs

The file is displayed in the **File name** text box.

5. Click **Next**. The **Select Dictionaries** dialog box displays.
6. Select the dictionaries to be imported, or click **Select All**.
7. By default, the Import/Export wizard imports only those dictionary words that you have not changed. To import the entire dictionary and overwrite your changes select **Import all words and overwrite any modifications**
8. Click **Next**. A summary screen displays that lists your selections.
9. Click **Finish** to import the dictionaries, or **Back** to change your settings.

Related topics

- *Adding a dictionary*, page 217
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Importing a unicode text file

Import a Unicode text file to create a new dictionary or to overwrite the contents of an existing dictionary.

Note

To create a new custom dictionary, see *Adding a dictionary*, page 217.

Creating the Unicode text file:

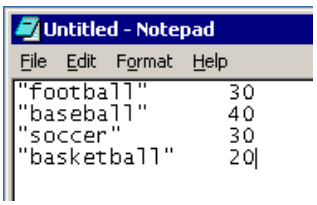
1. Open a text editor, such as Notepad.
2. Enter the words and scores in a list. The format must be

   “Word or Phrase”[tab space]Score

   Examples:

   “Football”[tab space]30

   “Baseball”[tab space]40



3. Save the file as file type Unicode.

> **Note**
> If the file is not saved as Unicode, the dictionary cannot be imported.

Importing the Unicode text file:

1. Open the **Dictionary Management** window.
   - If you intend to overwrite an existing dictionary, make sure you have selected the correct dictionary in the left panel.
   - If you are creating a new dictionary, select either **Websense Dictionaries** or **Custom Dictionaries** in the left panel.
2. Select **File > Import Unicode TXT file**.
3. Navigate to the Unicode file to import and click **Open**. The **Import Dictionary** dialog box displays.

   New – Creates a new dictionary under Custom Dictionaries.

   Overwrite – Overwrites the contents of the dictionary that you have selected in the left panel.
4. To import the Unicode file as a new dictionary, click **New**. You are prompted to give the new dictionary a name and description.
5. Click **OK**. The new dictionary displays in the Dictionary Management window.
6. To overwrite the dictionary that is currently selected, click **Overwrite**. The selected dictionary is replaced by the new dictionary.

If the file is not imported successfully, an error message displays. Check the format of the entries in the file and ensure that the file is saved as Unicode.

Related topics

- *Adding a dictionary*, page 217
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Exporting dictionaries

Use Dictionary Management to export dictionaries from Websense Email Security. Exporting dictionaries can be helpful if you are running multiple instances of Websense Email Security. By exporting a dictionary you have to edit it only once.

There are 2 ways to export dictionaries:

- As a Websense Email Security dictionary pack (an XML file). See *Exporting a dictionary pack*, page 225.
- As a Unicode file. See *Exporting a dictionary as a unicode file*, page 225.

You can export only one dictionary at a time to a Unicode file.

Related topics

- *Adding a dictionary*, page 217
- *Importing dictionaries*, page 222

Exporting a dictionary pack

To export a Websense Email Security dictionary pack:

1. Open **Dictionary Management**.
2. Select **File > Import/Export dictionary pack.** The Import/Export Utility wizard opens.
3. Click **Next**. The **Select Source and Target** dialog box displays.
4. Select **Export to file**.
5. Enter or browse to a name and location for the export file.

   By default, Websense dictionaries are located in the folder:
   Websense Email Security\Language Packs
6. Click **Next**. The **Select Dictionaries** dialog box displays.
7. Select the dictionaries to be exported, or click **Select All**.
8. Click **Next**. A summary screen displays that lists your selections.
9. Click **Finish** to export the dictionaries, or **Back** to change your settings.

Related topics

- *Adding a dictionary*, page 217
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

Exporting a dictionary as a unicode file

To export a dictionary as a Unicode file:

1. Open **Dictionary Management**.
2. Select a dictionary to export.
3. Select **File > Export Unicode file**.
4. The **Save As** dialog displays. Save the file as a Unicode file type. Either use the default file name, or enter a different file name.
5. Click **Save**. A message box confirms that the file was exported.

Related topics

- *Adding a dictionary*, page 217
- *Importing dictionaries*, page 222
- *Exporting dictionaries*, page 224

10 Scheduler

The Scheduler provides a flexible mechanism for managing the regular activities of Websense Email Security.

Use the Scheduler to:

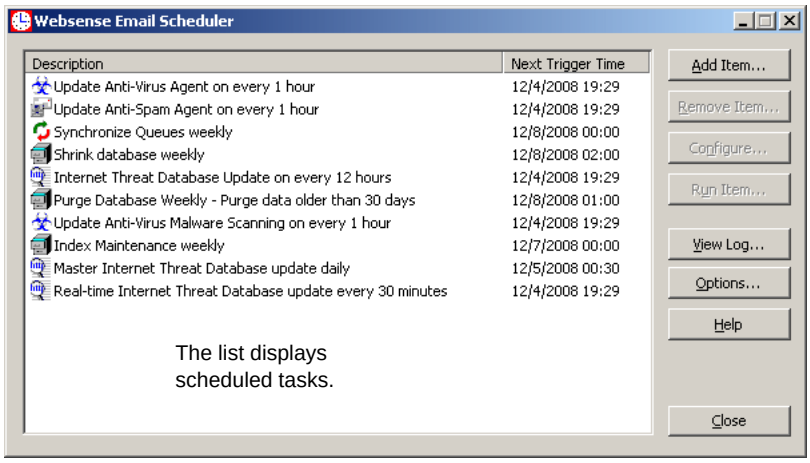
- Update tools that use Websense content, such as the Anti-Spam Agent, ensuring that Websense Email Security is armed with the most up-to-date information about new kinds of spam and other threats.
- Automatically manage email queues to avoid congestion and keep your system running efficiently.
- Manage the logging and configuration database.

Opening the Scheduler

To open the Scheduler select:

Start > **Programs** (or **All Programs**) > **Websense Email Security** > **Scheduler**

Scheduler window



Scheduled events

You can use the Scheduler to schedule the following events.

Event	What it does	Find out more
Anti-Spam Agent Update	Download the latest Anti-Spam Agent files.	*Scheduling Anti-Spam Agent updates*, page 229
Anti-Virus Agent Update	Download the latest Anti-Virus Agent files.	*Scheduling Anti-Virus Agent updates*, page 230
Anti-Virus Malware Scanning Live Update	Download the latest Anti-Virus Malware Scanning files.	*Scheduling Anti-Virus Malware Scanning updates*, page 230
Database Management	Purge, archive, rebuild, or shrink the logging database.	*Scheduling database management tasks*, page 234
Internet Threat Database Update	Download the latest Internet Threat Database files.	*Scheduling Internet Threat Database updates*, page 231
Queue Synchronization	Synchronize the database with the actual status of the server.	*Scheduling Queue Synchronization*, page 232

Default scheduled events

During installation, Websense Email Security automatically creates the following scheduled events.

Default Event	Time
Anti-Spam Agent Update	Daily – every hour, 7 days a week.
Anti-Virus Agent Update	Daily – every hour, 7 days a week.
Anti-Virus Malware Scanning Live Update	Daily – every hour, 7 days a week. **Note:** This event is not created automatically if you have *upgraded* from SurfControl E-mail Filter v5.2 or later.
Purge Database	Weekly – on Monday at 01:00. Purge data older than 30 days.
Shrink Database	Weekly – on Monday, 1 hour after purge.
Queue Synchronization	Weekly – on Monday at 02:00.
Database Index Maintenance	Weekly – on Sunday at 00:00.
Master Internet Threat Database Update	Daily – at 00:30, 7 days a week.
Real-time Internet Threat Database Update	Daily – every 30 minutes, 7 days a week.

Options for scheduled events

Using the **Options** button on the Scheduler window, you can set the following options for the scheduled events:

- **Database Query Timeout** – You can set a limit on the amount of time that the Database Management Archive task is allowed before it is stopped. See *Archiving a database*, page 235.
- **Notify System Administrator if a Scheduler event fails** – Use this to notify the administrator if a scheduled event fails. This is the address specified in the **Server Configuration** > **Administration** screen. See *Administration settings - general*, page 86.

Scheduling Anti-Spam Agent updates

Websense continually updates the Anti-Spam Agent files to ensure that you have the latest protection against spam. You should regularly update your Anti-Spam Agent to keep your system up-to-date.

To schedule Anti-Spam Agent updates:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Anti-Spam Agent Update** from the drop-down list.
3. Select the frequency of the update:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute
4. Enter a description in the **Description** field. This helps you to recognize this event in the Scheduler window.
5. Click **OK**.

The update event is listed in the Scheduler window.

Scheduling Anti-Virus Agent updates

Websense constantly updates the Anti-Virus Agent files to ensure that you have the latest protection against viruses. You should regularly update your Anti-Virus Agent to keep your protection up-to-date.

To schedule Anti-Virus Agent updates:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Anti-Virus Agent Update** from the drop-down list.
3. Select the frequency of the update:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute

   Note

   Websense recommends that you update the Anti-Virus Agent files every hour.

4. Enter a description in the **Description** field. This helps you to recognize this event in the Scheduler window.
5. Click **OK**.

The update event is listed in the Scheduler window.

Scheduling Anti-Virus Malware Scanning updates

Websense continually updates the Anti-Virus Malware Scanning files (the Authentium component of the Anti-Virus Malware Scanning object) to ensure that you have access to the latest protection against viruses. You should regularly update your Anti-Virus Malware Scanning tool to keep your system up-to-date with the latest protection.

To schedule Anti-Virus Malware Scanning updates:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Anti-Virus Malware Live Update** from the drop-down list.
3. Select the frequency of the update:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute

   > **Note**
   > Websense recommends that updates to the Anti-Virus Malware Scanning files are run every hour.

4. Enter a description in the **Description** field. This helps you to recognize this event in the Scheduler window.
5. Click **OK**.

The update event is listed in the Scheduler window.

Scheduling Internet Threat Database updates

Websense continually updates the ThreatSeeker Internet Threat Database files to ensure that you have access to the latest protection against Internet threats, such as email that contains links to inappropriate Web sites. You should regularly update your Internet Threat Database to arm your system with the latest protection.

There are 2 predefined, preconfigured Internet Threat Database update tasks:

- Master Internet Threat Database update
- Real-time Internet Threat Database update

Master Internet Threat Database update: This task downloads the most recent master database. Websense, Inc. updates the master Internet Threat Database several

times a week. The download may pull the full database, but more often it is packaged as an incremental update. By default, the task runs once a day.

Real-time Internet Threat Database update: This task downloads the most recent incremental update to the database. These real-time updates are released by Websense, Inc. several times a day, as needed. They are incremental updates and are usually quite small.

To create a new Internet Threat Database update task:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Internet Threat Database Update** from the drop-down list and click **Configure**. The **Select update event** dialog box displays.
3. Select **Master update** or **Real-time update** and click **OK**.
4. Select the frequency of the update:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute
5. Enter a description in the **Description** field. This helps you to recognize this event in the Scheduler window.
6. Click **OK**.

The update event is listed in the Scheduler window.

Scheduling Queue Synchronization

Note

You should schedule this event at a time when there is little or no traffic on the network.

The contents of the queues can sometimes be different from the email listed in the STEMLog database, for example if you delete email directly from the Queue folders.

The Queue Synchronization event synchronizes the two. This improves the performance of the Message Administrator and supports the use of multiple servers. It also maintains the integrity between database and email files so that they are unlikely to be lost. However, queue synchronization can also retrieve lost email.

Manage your queued email to avoid large numbers of delayed or isolated email. This reduces the time taken for queue synchronization to complete.

To schedule a Queue Synchronization event:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Queue Synchronization** from the drop-down list.
3. Select the frequency of the synchronization:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute
4. Enter a description in the **Description** field. This helps you to recognize this event in the Scheduler window.
5. Click **Configure**. The **Queue Synchronization** dialog box displays.
6. By default, all queues are synchronized. To *exclude* one or more queues from the synchronization, click **Add**. The **Add Queue** dialog box displays.
7. Select the queue that you *do not* want synchronized and click **OK**.

   Note
   You can only select one queue at a time.

8. Repeat the preceding steps for all of the queues that you *do not* want to synchronize. The excluded queues are shown in the **Exclude selected queues** list.
9. Set the maximum number of messages to be synchronized.

   Default = 10000
10. Click **OK** to return to the **Scheduler Item Configuration** dialog box.
11. Click **OK**.

The Queue Synchronization event is listed in the Scheduler window.

Scheduling database management tasks

> **Note**
> Websense Email Security services stop when database management tasks are running. Therefore, you should schedule these tasks at times of low email traffic so that they have minimal impact on your email system.

Websense Email Security continually records a log of all email traffic in your system and stores the data in a logging database. Because the size of this database increases very quickly, you should schedule regular database management tasks. You can automate the following tasks.

Task	Description
Purging a database, page 234	Deletes selected data from the database. You can select to purge all the logs, or the individual logs, such as Connection Log, Rules Log, and so on, from the database.
Archiving a database, page 235	Copies or moves selected data from the database to a specified file.
Shrinking a database, page 237	Reduces the size of the database by removing redundant space, but does not delete any data from the database.
Database Index Maintenance, page 238	Rebuilds indexes that become fragmented due to database activity (INSERTs, UPDATEs, and DELETEs).

Purging a database

The data you delete from the database will not be available for reports.

To delete data from the logging database:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Database Management** from the drop-down list.
3. Select the frequency of the task:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

Monthly – You can set either:

- A specific date in every month and the hour and minute on that date
- Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

Yearly – You can set either:

- A specific date in a specific month and the hour and minute on that date
- Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute

4. Enter a description in the **Description** field. This helps you to recognize this task in the Scheduler window.
5. Click **Configure** and then **Purge Database.** The **Purge** dialog box displays.
6. Select the log to purge from the database in this event:
   - All logs
   - Connection Log
   - Receive Log
   - Rules Log
   - Audit Log
   - Send Log
   - System Log
7. Select one option for the data to delete:
   - **Purge All** – Deletes all database entries.
   - **Purge data older than 24 hours**
   - **Purge data older than *n* days** – Deletes data older than the number of days that you set.
   - **Purge data older than date** – Deletes data older than the date you set.
   - **Purge Range** – Deletes data between the 2 dates you set.
8. To remove all email address data that is not currently being used by the database, select **Purge unused email address data**.

   Example: You might use this after your system has been subject to a large spam attack, which has filled the database.

   To remove all data that has not been synchronized by the reporting, select **Purge unsynchronized email address data**.
9. Click **OK** to return to the **Scheduler Item Configuration** dialog box.
10. Click **OK**. The Purge Database task is listed in the Scheduler window.

Archiving a database

You can copy or move all or specific data from a database into a specific file.

To archive the database:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Database Management** from the drop-down list.
3. Select the frequency of the task:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute
4. Enter a description in the **Description** field. This helps you to recognize this task in the Scheduler window.
5. Click **Configure** and then **Archive Database**. The **Archive** dialog box displays.
6. Select one option for the data to archive:
   - **Archive All** – Archives all database entries.
   - **Archive data older than 24 hours**
   - **Archive data older than N days** – Archives data older than the number of days you set.

     Note that with this option, the archive operation compiles message logs based on the specified date rather than on the hour of day that the archive request is scheduled. For example, if you use the **Archive Older Than 1 Day** option, and the archive activity is scheduled for noon Wednesday, the data in your archive will not contain message data from Tuesday, only for Monday and earlier.

     If you want data from Tuesday, you would choose the **Archive Older Than 0 Days** option to run at noon on Wednesday.
   - **Archive data older than date** – Archives data older than the date you set.
   - **Archive Range** – Archives data between the 2 dates you set.
7. **Archive to:**

   Enter or browse to the location of the archive file. The default archive folder is

   C:\Program files\Websense Email Security\Archive

   To automatically base the archive file name on the date that the archive is performed, select **Unique date-based filename**.

To delete the original data from the logging database, select **Purge Archived Data**.

8. Click **OK** to return to the **Scheduler Item Configuration** dialog box.
9. Click **OK**. The Archive Database task is listed in the Scheduler window.

Shrinking a database

Shrinking reduces the file size of the database by eliminating redundant space without removing any useful data.

To shrink the database:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Database Management** from the drop-down list.
3. Select the frequency of the task:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute
4. Enter a description in the **Description** field. This helps you to recognize this task in the Scheduler window.
5. Click **Configure** and then **Shrink**. The **Shrink/Compact Database** dialog box displays.
6. Specify the percentage of the current database size that you want to shrink the database to (between 1% and 99%).

   Default = 10% (of the current size)
7. Click **OK** to return to the **Scheduler Item Configuration** dialog box.
8. Click **OK**. The Shrink Database task is listed in the Scheduler window.

Database Index Maintenance

The Database Index Maintenance task defragments and rebuilds the STEMLog database indexes. This results in a faster, more reliable database. Due to continual use in the form of INSERT, UPDATE, and DELETE operations, over time the indexes become fragmented and the database becomes less efficient. The Database Index Maintenance task restores the database indexes to best efficiency.

By default, Database Index Maintenance is activated and scheduled to run every Sunday morning at midnight (00:00). The task needs no extra configuration; it is ready to run.

Should you decide to disable the task, for example because the system is very busy, you can remove the task or change its schedule. It is recommended, however, that you run the Database Index Maintenance task periodically to ensure best database performance.

To add a new Database Index Maintenance task:

1. In the Scheduler window click **Add Item**. The **Scheduler Item Configuration** dialog box displays.
2. Select **Database Management** from the drop-down list.
3. Select the frequency of the task:

   Daily – You can set either:

   - A specific time on one or more days, by selecting the days and then setting the hour and minute
   - A specific interval, by selecting the **Every HH:MM** check box, and then setting the interval in hours and minutes

   Weekly – You can set a specific day, and the hour and minute on that day.

   Monthly – You can set either:

   - A specific date in every month and the hour and minute on that date
   - Automatically at the end of the month, by selecting the **End of Month** check box, and then setting the hour and minute

   Yearly – You can set either:

   - A specific date in a specific month and the hour and minute on that date
   - Automatically at the end of a specific month, by selecting the **End of Month** check box, and then setting the hour and minute
4. Enter a description in the **Description** field. This helps you to recognize this task in the Scheduler window.
5. Click **Configure** and then **Index Maintenance**.
6. Click **OK** to return to the **Scheduler Item Configuration** dialog box.
7. Click **OK**. The Database Index Maintenance task is listed in the Scheduler window.

Event Log

To examine a log of Scheduler activities, click **View Log**. The **Scheduler Event Log** window displays and loads the current log file.

The log includes the date, timestamp, name of scheduled task, status (i.e., completed, failed), and descriptive information related to each recent event.

The current log file is grows until it reaches a 500 KB size limit, at which time the file is closed and a new file is created. As many as 5 log files are retained. When it is necessary to create a 6th log file, the oldest log file is deleted.

Click **Load All** to load the contents of all log files.

Click **Refresh** to load the contents of only the active log file.

Click **Close** to close the Log window.

11 Remote Administration

There are 2 facilities for administrating Websense Email Security from a remote computer:

- *Administration Client*, page 241
- *Web Administrator*, page 241

Administration Client

Note

When you install the Administration Client on remote computers, you can select the Websense Email Security components that you need to administrate. See the *Websense Email Security Installation Guide* for instructions.

Depending on the Websense Email Security components that you selected, using the Administration Client you have remote access to the following functions:

- Message Administrator – See *Message Administrator*, page 197.
- Rules Administrator – See *The Rules Administrator*, page 119.
- Monitor (including Server Configuration) – See *The Monitor*, page 97.
- Dictionary Management – See *Dictionary Management*, page 215.

You can also configure administrators. To set up remote users and specify their access permissions, see *Configuring administrators for remote access*, page 87.

Web Administrator

The Web Administrator enables you to access the following Websense Email Security functions from a remote computer:

- *Message Administrator*, page 243
- *Dictionary Management*, page 246

- *Viewing logs*, page 249

You can access all of these features from any Web Administrator screen.

Opening Web Administrator

You can open Web Administrator from either:

- The Websense Email Security server
- A remote computer

For both methods, the Web Administrator Start screen is displayed in your Web browser, see *Configuring administrators for remote access*, page 87.

Opening Web Administrator from the Websense Email Security server

To open Web Administrator from the Websense Email Security server, select

Start > **Programs** (or **All Programs**) > **Websense Email Security** > **Web Administrator**

Opening Web Administrator from a remote computer

Before you can use Web Administrator from a remote computer, you need to set up administrators in the Server Configuration console. The administrator's permission settings must include **Message Administration**. See *Configuring administrators for remote access*, page 87.

Enter the following address into your internet browser:

```
http://<IP address of Websense Email Security server>:<standard
port number>/index.htm.
```

For example, to access an installation on a server with an IP address of 172.22.9.73 and a standard port of 8181 specified during installation, the URL would be: http://172.22.9.73:82/index.htm

The log on screen displays.

Enter your username and password.

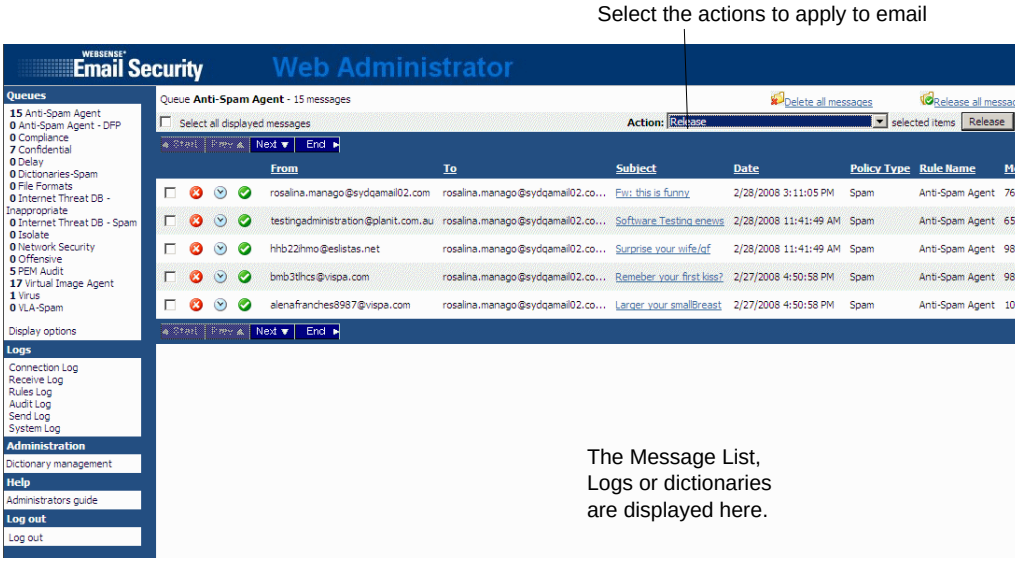
When you have logged on, the Web Administrator **Start** screen displays in your browser.

Note

You can access all of these features through any screen in the Web Administrator.

Message Administrator

Use the Message Administrator to manage email within queues.



See:

Sorting email, page 243

Moving, releasing and deleting email, page 243

Viewing email properties, page 244

Analyzing email, page 245

For more about working with email queues, see *Working with queues*, page 207.

Sorting email

To sort the list, click a column heading. For example, if you click the Subject heading once, the whole list is sorted by subject in descending order; click the column heading again to reverse the sort order.

Moving, releasing and deleting email

To move, release or delete any or all of the email in the list:

1. Select the check box of each email that you need.

   To select all email on the list, select the **Select all displayed messages** check box.
2. In the **Action** drop-down, select what you want to do with the selected email:
   - **Release** – Moves the email into the Send queue, which enables them to be sent to their destination.

- **Delete** – Deletes the email.

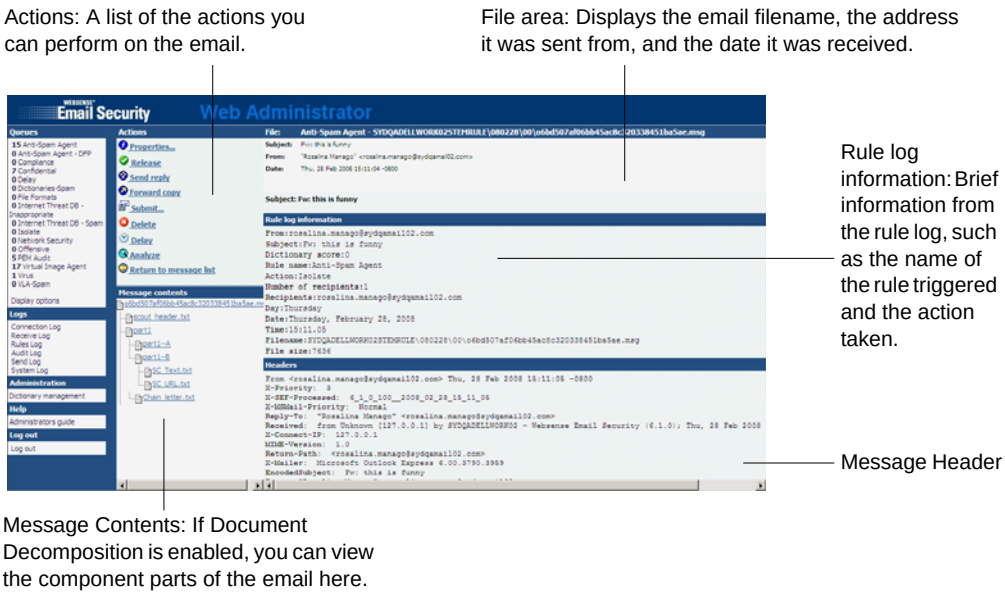
> **Note**
> You cannot retrieve deleted email.

- **Move** – Moves the email to another queue. Each queue is listed separately.

3. To complete the action, click the button next to the **Action** drop-down list.

Viewing email properties

Click an email to view its properties.



There are 5 activity and information areas:

Screen area	Description
Actions	Lists the actions you can perform on the email. See *Email actions*, page 245.
Message content	If Document Decomposition is enabled, you can view the component parts of the email here. See *Configuring Document Decomposition*, page 136.
File area	Displays the email filename, the address it was sent from, and the date it was received.
Rule log information	Brief information from the rule log, such as the name of the rule that triggered and the action taken.
Headers	Header details of the email.

Email actions

The actions you can perform on an email are listed in the **Actions** panel. These actions are the same as the actions in Message Administrator.

Action	Description
Properties	Shows information about the selected email, including details of recipients and file size.
Release	Place the email in the Send queue so that it can proceed to its destination.
Send reply	Send a reply to the sender of the email. An email form opens for you to type your text. You can either enter the text manually, or use pre-set text.
Forward copy	Forward a copy of the email to another user. You can enter an email address in the **To** field as well as using the check boxes to send the email to: • The message sender • The message recipient • The systems administrator
Submit	Report the email to Websense as Spam. Websense analyzes the email and any attachments for inclusion in the Anti-Spam Agent signature file.
Delete	Delete the email. You are asked to confirm your choice before the email is deleted.
Delay	Move the email into the delay queue. You are asked to confirm your choice before the email is delayed.
Analyze	Shows each word in the email that has triggered the dictionary rule, how often it occurs and its score.
Return to message list	Clears the email details screens and returns to the email list display.

Analyzing email

When you analyze an email, you can view each word that has triggered the dictionary rule, how often it occurs and its score. You can analyze any email. It does not need to have triggered a rule.

To analyze email:

1. Click **Analyze**. The **Analyze** page displays.
2. Select the dictionary to be used to analyze the email.

   The screen displays an analysis of the email, including
   - The words from the email that appear in the selected dictionary
   - The message part in which the words occur
   - The value assigned to each word
   - The number of these words found

- The individual word scores
- The total word score

3. From the **Message part** drop-down list, select the parts of the email to scan:
   - Entire Message
   - Header
   - Body
   - Attachments
4. From the **Scoring** drop-down list, select either:
   - **Threshold total** – If the email is in a multipart alternative format, you can display only the words from the part that scored highest.
   - **Grand total –** Display the dictionary scoring words from all selected parts of an email. In the case of multi-part alternative email, identical dictionary scoring words from alternative parts have a cumulative effect on the final score for the selected dictionary.
5. Click **OK** to return to the email list.

Dictionary Management

Use the Dictionary Management functions to create and edit dictionaries.

See:

Dictionary Management, page 215

Adding a dictionary, page 246

Adding words or phrases to a dictionary, page 247

Editing dictionary words, page 220

Deleting words from a dictionary, page 220

Deleting a dictionary, page 221

Adding a dictionary

To add a dictionary:

1. Open **Dictionary Management**.
2. Click the **New Dictionary** button  . The **Add/Edit dictionary** dialog box displays.
3. Name the new dictionary.
4. In the **Description** field, enter a description of the new dictionary.

5. If you want to display a warning message when the dictionary is opened (for example if the dictionary contains offensive words), enter a warning message in the **Warning Message** field and select **Display this message when dictionary launches**.
6. Click **OK**. The new dictionary displays under **Custom Dictionaries**. You can now select your dictionary when using the dictionary-based rules objects (e.g. the LexiMatch object).
7. Click  to save your changes.

Related topics

- *Adding words or phrases to a dictionary*, page 247
- *Editing dictionary words*, page 220
- *Deleting words from a dictionary*, page 220
- *Deleting a dictionary*, page 221

Adding words or phrases to a dictionary

Note

To use the Confidential dictionary in rules, you need to add the words and phrases that signify confidential content in your organization.

You can add words or phrases to a dictionary and give them a score. You can also use number pattern recognition, wildcards and/or binary sequences to make dictionary scanning tools more powerful.

Using number pattern recognition

You can add any pattern of numbers to a dictionary using the # character to signify a single number.

For example #### #### #### #### will find the credit card number 1234 5678 9011 1213, but not the string abcd 1234 defg 5678.

Using number pattern recognition can prevent email users from transmitting potentially sensitive data, such as credit card details, account numbers or patient file numbers.

Using wildcards

You can use wildcards to make the Websense Email Security dictionary scanner more extensive. With no wildcards, a word is assumed complete and separated by white space or punctuation marks. With wildcards, you can scan parts of words.

You can use the following wildcard characters.

> **Note**
> You cannot place one wildcard character immediately next to another.

Wildcard	Description
*	One or more characters at the beginning or end of a word or phrase. Example: sex* finds sexy or sexily, but not Essex.
?	A single character in a word or phrase. Example: jo?n would match john and joan, but not johann.
^	One or more white-space characters.
!	A single white-space or punctuation character.
\	An escape character.

Using Binary Sequences

You can also search for binary sequences. Use this ability to identify specific binary file sequences expressed as hexadecimal sequences.

To enter a binary sequence, enter **`~** followed by an even number of hexadecimal characters that represent the search sequence.

For example **`~61626364** is the Binary representation of abcd

A rule to detect this binary sequence would trigger if a email contained the following strings:

- abcd
- abcdxxxabcdxxx

The phrase **ABCD** would not trigger the rule because the binary code distinguishes between upper and lower case letters.

To add words or phrases to a dictionary:

1. Click the dictionary in the list. A screen shows the existing words and scores in the dictionary.
2. Click **Add new phrase**. The **Add phrase** screen displays.
3. Enter a word or phrase.
4. Enter a value between 0 and 100 for the word or phrase.

   The higher the score, the fewer instances of the word or phrase need to appear in an email to trigger a Dictionary Threshold rule.
5. Click **OK**. The word and its value are displayed in the dictionary.
6. To be able to use the word, click **Commit Dictionary Changes**.

Related topics

- *Adding a dictionary*, page 246
- *Editing dictionary words*, page 220
- *Deleting words from a dictionary*, page 220
- *Deleting a dictionary*, page 221

Viewing logs

You can view the following logs:

- **Connection log** – The connections from the host servers to Websense Email Security.
- **Receive log** – Messages that have been received by Receive Service.
- **Rules log** – Messages that have triggered a rule, including the rule name, policy type and the size of the email.
- **Audit log** – Actions that have been carried out on messages, including the audit user, audit type and activity for each email.
- **Send log** – Messages that have been received and released by the Send Service, including the route, IP address of the mail server, size of the email and the SMTP code.
- **System log** – All system activity.

Click a link to display the properties of an individual log.

12 Performance Monitoring

The Microsoft Windows Performance tool is very useful for monitoring statistics on the performance of your system and the volume of mail being processed.

To find out more about Performance, consult Windows Help and documentation.

Windows Performance monitoring

You can use the Windows Performance tool to monitor the performance of your system and display statistics on the volume of mail being processed.

To use the Windows Performance tool:

1. In your operating system screen, select:

   Start > Settings > Control Panel > Administrative Tools > Performance

   The Performance console displays.
2. In the navigation panel, select **System Monitor**.

   The system activity displays in the right-hand panel.
3. Right-click anywhere in the right-hand panel.

   A shortcut menu displays.
4. In the shortcut menu, select **Add Counters**. The **Add Counters** dialog box displays.
5. To count the number of messages processed, select the computer where Websense Email Security is installed.
6. Select Websense Email Security from the **Performance object** drop-down list.
7. Select the types of counters to be used to monitor your system. For a description of a counter, select the counter in the list and click **Explain**.
8. Click **Add** to add the counters to the Performance tool.
9. The counters are displayed in the lower right-hand panel of the **Performance** console.

13 Virtual Learning Agent

The Virtual Learning Agent (VLA) is a flexible tool that you train to identify specific types of content that your organization wants to protect, such as confidential information.

The VLA consists of two components:

- The **Virtual Learning Agent Training Wizard**: The Training Wizard is what you use to train the VLA to recognize certain types of content. Use the Training Wizard to specify the categories of information you want to detect.
- The **Virtual Learning Agent object** is a What object that you include in rules using the Rules Administrator. The Virtual Learning Agent object uses information from the Virtual Learning Agent to detect content that matches the categories you specify.

In addition to the VLA reference material, there is a *VLA tutorial*, page 264 that walks you through the process of setting up and training the VLA. After doing the tutorial, you will be ready to use your own information to train the VLA and effectively include it in a rule.

The example used in the tutorial is the creation of a category called **Confidential Travel.** All of the material that you need to create the category is provided with Websense Email Security and is located in:

Websense Email Security\Resources\VLA Examples

Related topics

- *Workflow*, page 253
- *Source Documents*, page 254
- *Training the VLA*, page 255

Workflow

Before you can use the VLA object in a rule, you must train it to recognize the kind of content you want to detect. Before you can train the VLA you need to consider the categories of content you want to protect and gather representative source material to perform the training.

When that work is done you're ready to use the VLA Training Wizard to add your categories and train the VLA. The VLA Training Wizard automatically works through the setup and training process using the information and materials you supply.

The VLA Training Wizard includes the following steps:

- Adding a category name and description.
- Adding documents to the category.
- Adding documents to the counter category.
- Training the VLA.
- Testing the VLA using additional documents.

Related topics

- *Source Documents*, page 254
- *Training the VLA*, page 255
- *VLA tutorial*, page 264

Source Documents

Before you create a new VLA category, you need to gather a set of training and testing documents. The best files to use are documents such as Word files, Excel workbooks, PDFs, or PowerPoint presentations. You can also use email, but because of the extra data contained in the email header file, it could take longer to train the VLA and to choose keywords.

Training Documents – The VLA uses training documents to learn about the content in the category.

To create and train a new category you need to collect:

- 10-20 messages or documents that contain content that describes the category you want to create.
- 10-20 messages or documents that contain content that does not describe the new category. These are added to the counter category.

Testing Documents – After you have trained the VLA, you need to test it to check that it can identify content from your category accurately enough to be used in rules. You will need:

- 10-15 additional category documents or messages that can be used to test the VLA to check that it can correctly identify content belonging to the category.
- 10-15 additional counter category documents or messages.

Whenever you add a new VLA category, you should review the counter-category documents and keywords to make sure that the counter category does not contain any keywords that might belong to the new category.

If you plan to do the VLA tutorial to create the sample category Confidential Travel, all the files you need are supplied in the sub-folders of: **Websense Email Security > Resources > VLA Examples > Confidential Travel Training**.

Related topics

- *Workflow*, page 253
- *Training the VLA*, page 255
- *VLA tutorial*, page 264

Training the VLA

To train the VLA in your chosen category, follow these steps.

1. Collect your source documents.
2. Add the category training files to the VLA.
3. Choose keywords from the category training files.
4. Add category test files.
5. Add counter category training files to the VLA.
6. Choose counter category keywords from the counter category training files.
7. Add counter-category test files.
8. Train the VLA.
9. Test the VLA.
10. Check that the VLA is accurate enough to use in rules to detect your chosen category.
11. Create rules using the Virtual Learning Agent object.

Related topics

- *VLA tutorial*, page 264
- *VLA categories*, page 256
- *VLA counter categories*, page 258
- *Processing training files*, page 261

Starting the VLA Training Wizard

To open the VLA Training Wizard, select:

Start > Programs (or **All Programs**) **> Websense Email Security > Virtual Learning Agent**

The VLA Training Wizard Welcome Screen shows you:

- Existing categories you have configured, with their descriptions

- The accuracy of each category

Click **Next** to begin training the VLA.

Related topics

- *VLA tutorial*, page 264
- *VLA categories*, page 256
- *VLA accuracy*, page 263

VLA categories

You can train the VLA to recognize documents pertaining to a specific subject, for example a business project, travel and tourism, or health-related topics.

The key to successful use of the VLA is:

- Defining a category that is specific to your needs
- Training the VLA to recognize material that fits the category
- Training the VLA to recognize material that does not match the category (a counter-category)

You can train as many categories as you want in the VLA, making each category as specific as possible. This provides maximum accuracy, as well as the most useful logging and feedback.

Related topics

- *VLA tutorial*, page 264
- *The VLA Category Wizard*, page 257
- *VLA counter categories*, page 258

Configuring VLA categories

The **Configure VLA Categories** screen is used to create and manage VLA categories.

To create a new category:

1. Click **Add**. The **VLA Category Wizard** opens and guides you through the category setup process. When the VLA Category Wizard is complete, you are returned to the Configure Categories screen.
2. Click **Next**.

To configure an existing category:

Select the category and click **Configure**. The **VLA Category Wizard** opens and guides you through the process.

To remove a category:

Select the category and click **Remove**. Click **Yes** to confirm the action.

Related topics

- *VLA tutorial*, page 264
- *The VLA Category Wizard*, page 257
- *VLA counter categories*, page 258

The VLA Category Wizard

The first screen of the VLA Category Wizard is where you define the name of your category.

Fill in the fields as follows:

Category Name – Enter the name of your category.

Description – Enter a brief description of your category.

If you are configuring an existing category, the Name and Description fields are already filled in. You can edit the name and description of the category.

Related topics

- *VLA tutorial*, page 264
- *Adding category training files to the VLA*, page 257

Adding category training files to the VLA

The **Add Training Files** screen is used to add the source files you have gathered that the VLA will use to learn about the category.

1. Click **Add**. The **Add Files** dialog displays.
2. Navigate to the files you want to add.
3. Click **Open**. The **Add Files** dialog closes and the files are displayed in the **Add Training Files** screen.
4. Click **Next** to proceed.

Related topics

- *VLA tutorial*, page 264
- *Choosing category keywords*, page 257

Choosing category keywords

The Choose Keywords screen is where you pick out the words from your training files that most accurately represent the category you are training the VLA to recognize.

All the words from the training files are displayed in the left window. You can display the words in alphabetical order by clicking the **Word** column head. Alternatively, display the words in order of frequency by clicking the **Count** column head.

1. Select the words from the list that are relevant to your category, and click **Add**. If you change your mind and want to remove a word, highlight it and click **Remove**.
2. If you are re-training an existing category, you can choose to view only words from the training files you have just added. Select **Show New Only**.
3. You can exclude words from the training process by designating them Trivial Words.
4. When you have chosen your Keywords, click **Next** to continue configuring your category.

Related topics

- *VLA tutorial*, page 264
- *Adding category test files*, page 258

Adding category test files

Category test files are files containing similar content to the training files. The VLA uses these files to test how accurate it is in categorizing content as belonging to your category.

To add testing files:

1. On the **Add Testing Files** screen, click **Add**. The **Add Files** dialog box displays.
2. Navigate to the files you want to use as test files.
3. Select the files and click **Open**. The **Add Files** dialog closes and your chosen test files are displayed in the **Add Testing Files** window.
4. Click **Next**. The final screen of the **VLA Category Wizard** displays.
5. Click **Finish**.

Related topics

- *VLA tutorial*, page 264
- *VLA counter categories*, page 258

VLA counter categories

The VLA uses a counter-category built from documents and keywords that do not contain content belonging to the categories you are training the VLA to recognize.

Just as the VLA training categories must contain documents and keywords relevant to the category, the counter category must contain as many documents and keywords as

possible that are not relevant to any of the categories, as well as those that appear in multiple categories.

Creating a counter-category is an important step in achieving the level of accuracy needed to use the VLA object in rules.

When you are collecting training and testing files for the counter-category, you should look for legitimate business email and documents that do not apply to the category you are creating.

For more information about the Virtual Learning Agent and a tutorial, see *Virtual Learning Agent*, page 253.

Related topics

- *VLA tutorial*, page 264
- *Counter category*, page 259
- *Define counter examples*, page 259

Counter category

The VLA only uses one counter category. It must not contain any material that is representative of any VLA category. Therefore, when you create a new category, it is important that you review the details of the counter category.

Related topics

- *VLA tutorial*, page 264
- *Define counter examples*, page 259

Define counter examples

The **Define Counter Examples** screen displays how many counter example training and testing files have been added to the VLA.

Click **Configure** to add counter example testing and training files. The **Counter Category Wizard** opens.

When you finish adding your counter category files, you are returned to this screen.

Click **OK** to begin the training process.

Related topics

- *VLA tutorial*, page 264
- *VLA Counter Category Wizard*, page 260

VLA Counter Category Wizard

The **VLA Counter Category Wizard** takes you through the process of adding counter examples to the VLA.

Related topics

- *VLA tutorial*, page 264
- *Adding counter category training files to the VLA*, page 260

Adding counter category training files to the VLA

The **Add Counter Category Training Files** screen is used to add files that the VLA uses to learn about the counter category. The counter category training files contain content that is different from your VLA category.

Follow these steps:

1. Click **Add**. The **Add Files** dialog displays.
2. Navigate to the counter category files you want to add.
3. Click **Open**. The **Add Files** dialog closes and the files are displayed in the **Add Counter Category Training Files** screen.
4. Click **Next** to proceed to the next step.

Related topics

- *VLA tutorial*, page 264
- *Choosing counter category keywords*, page 260

Choosing counter category keywords

The **Counter Category Choose Keywords** screen is where you pick out the words from your training files that do not represent the category you are training the VLA to recognize.

All the words from the training files are displayed in the left window. You can display the words in alphabetical order by clicking the **Word** column head. Alternatively, display the words in order of frequency by clicking the **Count** column head.

1. Select those words from the list that are not associated with your category, and click **Add**. If you change your mind and want to remove a word, highlight it and click **Remove**.
2. If you are re-training an existing category, you can choose to view only words from the training files you have just added - select **Show New Only**.
3. You can exclude words from the training process by designating them Trivial Words. See *Trivial words*, page 264.

4. When you have chosen your Counter Category Keywords, click **Next** to continue configuring the Counter Category.

> **Note**
> The VLA uses a single Counter Category against all the categories you configure. So if you have more than one category configured, you need to check that the words in the Counter Category do not match any of the Categories

Related topics

- *VLA tutorial*, page 264
- *Adding counter category testing files*, page 261

Adding counter category testing files

Counter category test files are files containing similar content to the counter category training files. The VLA uses these files to test how accurate it is in categorizing content that belongs to your category.

To add counter category test files:

1. On the **Add Counter Category Testing Files** screen click **Add**. The **Add Files** dialog box displays.
2. Navigate to the files you want to use as counter category test files.
3. Select the files you want to use, and click **Open**. The **Add Files** dialog closes and the chosen test files are displayed in the **Add Counter Category Testing Files** window.
4. Click Next. The final screen of the VLA Category Wizard displays.
5. Click Finish.

Related topics

- *VLA tutorial*, page 264
- *Processing training files*, page 261

Processing training files

The **Training VLA** screen displays the progress of the VLA in learning about the category using the files you provided.

The progress bar shows how many files have been processed.

The pass number box displays.

The network accuracy displays.

When the VLA has finished training, click **Next** to begin testing the VLA.

Related topics

- *VLA tutorial*, page 264
- *Testing the VLA*, page 262

Testing the VLA

The VLA tests itself by examining all of the testing files and categorizing them as:

a. Belonging to your category.
b. Not belonging to your category.
c. Belonging to neither category.

It then assesses how many of the files it has categorized correctly and gives a percentage score that you can use to judge whether the VLA is accurate enough to be used in a rule.

When the progress bar reaches 100%, click **Next** to continue. The Testing Results screen displays.

Related topics

- *VLA tutorial*, page 264
- *VLA test results*, page 262
- *VLA accuracy*, page 263

VLA test results

The **Testing Files Results** screen shows a breakdown of how the VLA categorized the testing files. It shows the following columns:

- **File Name**

  A green check next to the filename means the VLA has correctly categorized the file.

  A red exclamation mark next to the filename means the VLA has incorrectly categorized the file.

  Click the **File Name** column heading to sort the test results in filename order.

- **Folder**

  The location of the testing files. Click the **Folder** column heading to sort the results in folder order.

- **Set Category**

  The category you specified the training file as belonging to.

- **Predicted Categories**

The category that the VLA classifies the file as belonging to, based on its training.

Related topics

- *VLA tutorial*, page 264
- *Training complete*, page 263
- *VLA accuracy*, page 263

Training complete

When you are satisfied with the accuracy of the VLA in detecting your category, you can use the Virtual Learning Agent Object in rules to filter email for content in that category.

Related topics

- *Virtual Learning Agent object*, page 179
- *Virtual Learning Agent*, page 253

VLA accuracy

The VLA trains itself by categorizing the testing files and measuring how many of the files it categorized correctly as belonging to the new category. The VLA then displays a percentage score that you can use to determine whether the VLA has been trained enough to be incorporated into rules. The table explains how to interpret the VLA accuracy score.

Score	What it means
85% or higher	You can confidently use this VLA category to build rules.
65% – 85%	This is acceptable, but you could increase accuracy by: • Selecting additional training documents • Reviewing all keywords
Less than 65%	This VLA category is not accurate enough to be used in rules. You should retrain the VLA until you get a higher rating for the category. To increase the accuracy: • Review your training files to make sure they accurately represent the category. • Review the counter-category training files to make sure they do not represent the category. • Review the keywords for the categories and counter-categories.

Related topics

- *VLA tutorial*, page 264
- *VLA categories*, page 256

Trivial words

Trivial words are words that can be found in documents of all types and categories. Therefore, trivial words cannot be used to by the VLA to evaluate whether an email belongs to a category. The VLA ignores trivial words.

The VLA has a predefined list of common trivial words such as “and”, “but”, “because”, and so on. You can add more trivial words to this list when you are selecting keywords.

To add trivial words to the VLA:

1. In either of the **Choose Keyword** screens, click **Trivial Words**.
2. You can add words from the word list or enter them individually.
   a. Select the words to be added to the trivial word list and click **Exclude**.
   b. Or click **New**, enter a word and click **OK**.

The words are removed from all word lists, including the current list displayed.

Related topics

- *Virtual Learning Agent*, page 253
- *VLA tutorial*, page 264

VLA tutorial

The VLA Training Wizard tutorial is designed to show you how to train the VLA by creating a sample category called **Confidential Travel**. The aim of this category is to detect any leak of information about a top-secret overseas business project.

When you installed Websense Email Security, a folder was created containing all the training and testing files you need to complete the tutorial. These documents are in the folder: **Websense Email Security\Resources\VLA Examples**

As you work through the tutorial, the VLA Wizard moves through these steps:

1. Adding a category name and description.
2. Adding positive documents to the category.
3. Adding counter documents to the category.
4. Training the VLA.
5. Testing the VLA using additional documents.

Let’s begin.

VLA Tutorial Step 1: Starting the wizard

1. To start the VLA Training Wizard, from the **Start** menu select

Programs (or **All Programs**) > **Websense Email Security** > **Virtual Learning Agent**

The Welcome screen displays. If the VLA has never been used, the **Trained Categories** list is empty.

1. In the Welcome screen, click **Next.** The **Configure VLA Categories** screen displays.
2. Click **Add**. The **Add Category Wizard** screen displays.

VLA Tutorial Step 2: Add Category Wizard

The **Add Category Wizard** prompts for a name and description of the new category.

1. Enter:
   - **Category Name** = Confidential Travel
   - **Description** = Sample Websense VLA Category
2. Click **Next** to move to the next step.

VLA Tutorial Step 3: Add positive categories

The **Add Training Files** screen displays. This is where you select the first group of positive documents or email that define the content of the Confidential Travel category.

1. Click **Add** to select the training files. The Add Files dialog box displays. It defaults to the Websense Email Security folder.
2. To navigate to the example training documents, select **Resources** > **VLA Examples** > **Confidential Travel Training**
3. Change the **Files of Type** to **All Files (*.*)** and select all the files in the folder.
4. Click **OK**. You are returned to the **Add Training Files** screen and the selected files are displayed.
5. Click **Next** to move to the next step.

VLA Tutorial Step 4: Choose keywords

After a few seconds of processing, the **Choose Keywords** screen displays.

1. Select the keywords that identify content that belongs to the new category.

   Select the keywords from the left panel and click **Add**.

   To select multiple keywords, use Shift or Ctrl.

   The selected words are marked in the left panel and displayed in the right panel.

   For a list of keywords for this tutorial, see *Confidential Travel keywords*, page 268.

   For details of trivial words, see *Trivial words*, page 264.

2. Click **Next** to move to the next step.

VLA Tutorial Step 5: Add testing files

In the **Add Testing Files** screen you add files similar in content to the positive training files. These files are used to test the accuracy of the category. These files are different from the training files but should contain similar content.

1. On the **Add Testing Files** screen click **Add**. The **Add Files** dialog box displays.
2. Navigate to the **Confidential Travels Test** folder.

   Websense Email Security\Resources\VLA Examples\Confidential Travel Test
3. Change the **Files of type** to **All Files (*.*)** and select all the files in the folder. The files are displayed in the **Add Testing Files** screen.
4. Click **Next** to move to the last screen in the Category Wizard.

VLA Tutorial Step 6: Define counter examples

The **End of VLA Category Wizard** screen displays.

1. Click **Finish**. You are returned to the **Configure VLA Categories** screen that was displayed in step 1, but this time the Confidential Travel category is listed in the window.
2. Click **Next**. The **Define Counter-Examples** screen displays. This is where you define content that is *not* a match for the Confidential Travel category.
3. Click **Configure** to start the **VLA Counter Category** wizard.
4. Click **Next**.
5. In the **Add Counter Category Training Files** screen, specify the files to use to teach the VLA what is *not* in the Confidential Travel category.
6. Click **Add**. The **Add Files** dialog box displays.
7. Open the **Non-Travel Training** folder.

   Websense Email Security\Resources\VLA Examples\Non-Travel Training
8. Change the **Files of type** to **All Files (*.*)** and select all the files in the folder. The files are displayed in the **Add Counter Category Training Files** screen.
9. Click **Next**.

VLA Tutorial Step 7: Choose counter category keywords

The **Counter Category Choose Keywords** screen displays. This is where you choose keywords that *do not* match the Confidential Travel category.

1. Click the Work column heading to sort the list alphabetically.
2. Select the keywords in the left panel and click **Add**. To select multiple keywords, use Shift or Ctrl.

For a list of keywords for this tutorial, see *Confidential Travel keywords*, page 268.

3. Click **Next** to move to the next step.

VLA Tutorial Step 8: Add counter category testing files

1. In the **Add Counter Category Testing Files** screen, add the files that the VLA will use to test itself. These test files are different from the training files but should contain similar content.
2. Click **Add**. The **Add Files** dialog box displays.
3. Open the **Non-Travel Test** folder.

   Websense Email Security\Resources\VLA Examples\Non- Travel Test
4. Change **Files of type** to **All Files (*.*)** and select all the files in the folder. The files are displayed in the **Add Counter Category Testing Files** screen.
5. Click **Next**.
6. Click **Finish**.

VLA Tutorial Step 9: Review the training and test files

The Confidential Travel category is listed in the **Configure VLA Categories** screen.

1. Click **Next**. The details of the counter-examples are displayed in the **Define Counter-Examples** screen.
2. Click **Next**.

VLA Tutorial Step 10: Training the VLA

A message displays that confirms that you have saved your work to this point and can begin training the VLA.

1. Click **OK** in the confirmation message to start training the VLA. The **Training VLA** screen displays a progress bar for training files processed.
2. When the training is complete, a message box displays. Click **OK**.
3. Click **Next** to start testing the VLA.

VLA Tutorial Step 11: Testing the VLA

The **Testing** screen displays. Testing ensures that the category is accurate enough to use in the rules. The VLA tests itself by examining all the testing files and categorizing them as:

   a. Belonging to the Confidential Travel category
   b. *Not* belonging to the Confidential Travel category
   c. Belonging to neither category

It then assesses how many of the Confidential Travel files it has categorized correctly and gives a percentage score that you can use to judge whether the VLA is accurate enough to use in a rule.

The **Testing** screen shows the progress of the testing process.

When the progress bar shows 100%, click **Next**.

VLA Tutorial Step 12: Testing files results

The **Testing Files Results** screen shows how many testing files the VLA has categorized as correctly belonging to the new category.

- Correctly categorized files = ✔
- Incorrectly categorized files = ❗

Click **Next**.

VLA Tutorial Step 13: Category addition complete

The **VLA Training Completed** screen displays the accuracy score of the category and the counter category. See *VLA accuracy*, page 263 for an explanation of the accuracy score.

Click **Finish**.

You have finished setting up the Confidential Travel VLA category.

Before you can use the new category in Rules, you need to restart the Rules service. In the message that asks if you want to restart the Rules service, click **Yes**.

If you open Rules Administrator and view the Virtual Learning Agent Object dialog box, you will see the Confidential Travel category available for selection.

This concludes the VLA Training Wizard tutorial.

Confidential Travel keywords

If you are creating the sample category Confidential Travel, you should select the keywords listed below for the category and the counter category.

Sample category keywords:

accommodation	boeing	expedia	navigant	room	travelodge
air	carriage	fare	nights	ryanair	trip
airfare	conditions	fares	open	seat	vacation
airline	confirmation	flight	passenger	seattle	valid
airlines	connect	flights	passengers	stansted	world

airport	deals	hotel	photo	terminal	
baggage	departure	hotels	receipt	ticket	
banners	destinations	international	refund	tickets	
board	domestic	london	reservation	transfer	
boarding	europe	miles	reservations	travel	

Sample counter category keywords:

account	customer	job	original	products	technology	virus
agent	database	letters	path	resources	terms	checked
apply	days	manager	permanent	rules	training	ware
checked	filtering	manutd	phone	salary	unknown	work
columbia	following	news	plain	security	users	writer
connect	individual	newsletter	plugin	server	virtual	years
cost	investment	number	product	software	terms	

14 Database Tools

Websense Email Security uses several databases to perform its tasks. There are 3 database tools for working with these databases. They are:

- *Configuration database management*, page 271

  This tool allows you to:

  - Back up the configuration database
  - Restore a previously backed up configuration database
- *Log database management*, page 273

  This tool allows you to:

  - Create a new log database
  - Back up the log database
  - Restore a log database backup file
  - Delete a log database
  - Truncate the log database transaction log
- *SQL user management*, page 277

  This tool allows you to set up and manage the SQL user accounts that are used to access the configuration and log databases.

Opening database tools

To open database tools select:

Start > **Programs** (or **All Programs**) > **Websense Email Security** > **Database Tools**

Select the database tool that you need. Each tool has a wizard.

Configuration database management

The Configuration database stores the details of Websense Email Security server setup and configuration options. Use the Configuration database management tool to:

- Back up the configuration database

- Restore a previously backed up database

Backing up the configuration database

It is useful to make a backup of your Websense Email Security system configuration to enable you to:

- Replicate the same configuration on each Websense Email Security server in your organization
- Restore your configuration if you need to reinstall Websense Email Security

To back up the configuration database:

1. From the Database Tools menu, select **Configuration Database Management**. The Configuration Database wizard opens.
2. Select **Backup database to a file**. The **SQL/MSDE Server details** screen displays.
3. Specify the location of the server that contains the database to be backed up.

   To connect to the server through a trusted connection, select the **Use trusted connection** check box.

   To connect to the server using the username and password you specify, clear the **Use trusted connection** check box and enter the username and password.
4. Click **Next**. The **Configuration Database Backup Details** dialog box displays.
5. Select the database from the drop-down list.

   Default = STEMConfig
6. Enter or browse to the location of the file where the database is to be saved.

   Default = Program files\Websense Email Security\Database\STEMConfig_<date>.bak
7. Click **Next**. A summary of your options displays.
8. If you need to change any details, click **Back**. If the options are correct, click **Next**.
9. A progress bar displays. A confirmation screen displays when the backup is complete. Click **Finish**.

Restoring the configuration database

You can restore a previous backup file to the configuration database. If you do this, your current configuration settings are replaced by those specified in the backup file.

To restore the configuration database:

1. From the Database Tools menu, select **Configuration Database Management**. The Configuration Database wizard opens.
2. Select **Restore Database from a File** and click **Next**. The **Restore Details** screen displays.
3. Select the backup file to restore. By default, this is the most recent backup file you created.

4. Select the database to restore.

   Default = STEMConfig

5. Click **Next**. A summary of your options displays.
   - If the options are correct, click **Next**.
   - If you need to change any details, click **Back**.
6. When the database has been restored, you need to stop and restart the Websense Email Security services.
   - To restart the Websense Email Security services immediately after the database has been restored, select **Restart Websense Email Security Services Now**.
   - To restart the Websense Email Security services manually at a later time, select **Restart Websense Email Security Services Later**.

Log database management

The log database records the details of email passing through Websense Email Security, as well as how Websense Email Security handles email that triggers rules.

You can use the Log Database Management tool to:

- Create a new log database
- Archive the log database
- Restore a log database backup file
- Delete a log database
- Truncate the log database transaction log

Creating a new log database

To create a new log database:

1. From the Database Tools menu, select **Log Database Management**. The Log Database Management wizard opens.
2. Select **Create a new log database** and click **Next**. An **MSDE/SQL Server Details** screen displays. Enter the server connection details.
3. From the **Server name** drop-down list, select the server that contains the database.

   You can connect to the server using:
   - A trusted connection
   - A username and password you supply
4. Click **Next**. A second **MSDE/SQL Server Details** screen displays. Enter the database details.
5. Enter a name and a DSN name for your new database. The database name must be different from the name of your existing database.

File location:

- To use the default file location, select the **Use default file location** check box and click **Next**.
- To specify file locations, clear the **Use default file location** check box, click **Next** and enter the database and transaction log file names. Click **Next**.

Set new database as the default:

- To use the existing data source with the new database, select the **Set the new database as the default database** check box.
- To specify a different data source, clear the **Set the new database as the default database** check box and enter the new DSN in the **New DSN Name** field.

6. A summary of your options displays.
   - If you need to change any details, click **Back**.
   - If the options are correct, click **Next**.
7. A confirmation screen displays when the new log database has been created. Click **Finish**.

Archiving the log database

To archive the log database to a file:

1. From the Database Tools menu, select **Log Database**. The Database wizard opens.
2. Select **Archive the log database to a file** and click **Next**. The **MSDE/SQL Server Details** screen displays.
3. From the **Server** drop-down list, select the server that contains the log database.
4. Connect to the server using either:
   - A trusted connection
   - A username and password you supply
5. Click **Next**.
6. Select the log database to archive.
7. Browse to the location where you want the archive file to be stored and click **Next**.
8. A summary of your options displays.
   - If the options are correct, click **Next**.
   - If you need to change any details, click **Back**.
9. A confirmation screen displays when the log database has been successfully archived. Click **Finish**.

Restoring an archived log database

To restore a database you have previously backed up:

1. From the Database Tools menu, select **Log Database**. The Database wizard opens.
2. Select **Restore Archived Log Data to a Database** and click **Next**. The **Configuration Database restore Details** screen displays.
3. Select the SQL database in which to restore the archived data.
4. Enter or browse to the log file to be restored, and select the database into which to restore it.
   - To restore the archived file to the file location specified in the archive file, select the **Use original file location** check box and click **Next**.
   - To specify a file location, clear the **Use original file location** check box and click **Next**. Enter:
     - The file location that the archived file will be restored to.
     - The file location of the transaction log.

     If you are restoring a large database, make sure you specify a location that has enough disk space to hold the restored database.

     - Click **Next**.
5. A summary of your options displays.
   - If you need to change any details, click **Back**.
   - If the options are correct, click **Next**.
6. A confirmation screen displays when the archived data has been successfully restored to the database.

   You need to stop and restart the Websense Email Security services:
   - To restart the Websense Email Security services immediately after the database has been restored, select **Restart Websense Email Security Services Now**.
   - To restart the Websense Email Security services manually later, select **Restart Websense Email Security Services Later**.
7. Click **Finish**.

Deleting a log database

To delete a log database:

1. From the Database Tools menu, select **Log Database**. The Database wizard opens.
2. Select **Delete an Existing Log Database** and click **Next**.
3. The **MSDE/SQL Server Details** screen displays. From the **Server** drop-down list, select the server that contains the database.

   You can connect to the server using:

   - A trusted connection
   - A username and password you supply

   Click **Next**.
4. The **Specify MSDE/SQL Server File Locations** screen displays.
5. Select the database to be deleted and click **Next**.
6. A summary of your options displays.
   - If the options are correct, click **Next**.
   - If you need to change any details, click **Back**.
7. A confirmation screen displays when the database has been deleted.
8. Click **Finish**.

Truncating the log database transaction log

The log database transaction log can grow very quickly, which can affect performance. To prevent this from happening, you can truncate it.

To truncate the log database transaction log:

1. From the Database Tools menu, select **Log Database**. The Database wizard opens.
2. Select **Truncate the log database transaction log** and click Next. The **MSDE/SQL Server Details** screen displays.

   From the **Server** drop-down list, select the server that contains the database.

   You can connect to the server using:

   - A trusted connection
   - A username and password you supply

   Click **Next**.
3. The **Specify MSDE/SQL Server File Locations** screen displays.

   Select the database that contains the transaction log.

   Default = STEMLog.

   Click **Next**.
4. A summary of your options displays.

- If you need to change any details, click **Back**.
- If the options are correct, click **Next**. A progress bar displays.

5. A confirmation message displays when the transaction log has been truncated successfully.
6. Click **Finish**.

SQL user management

Websense Email Security must be able to read and write to the logging and configuration databases. To access these databases it uses SQL User Accounts. The SQL User Management Tool enables you to set up and manage these accounts.

To manage the SQL/MSDE User account used by Websense Email Security, you can:

- Create a new SQL user account
- Change the password on a SQL user account
- Delete a SQL user account

Creating a new SQL user account

To create an new account:

1. From the Database Tools menu select **SQL User Management**. The **SQL User Management Welcome** screen displays.
2. Select **Manage an MSDE/SQL Server User Account** and click **Next**. The Manage an MSDE/SQL Server User Account screen displays.
3. Select **Create a SQL User account** and click **Next**. The **MSDE/SQL Server Details** screen displays.
4. Select the server that contains the database.
5. Connect to the server using either:
   - A trusted connection
   - A username and password you supply

   Click **Next**.
6. The **Create a SQL User Account** screen displays.
7. Enter the user name, password and password confirmation.
8. Click **Next**. A summary of your options displays.
   - If you need to change any details, click **Back**.
   - If the options are correct, click **Next**. A progress bar displays.

   A confirmation message displays when the Database wizard has created the new account.
9. Click **Finish**.

Changing the password on a SQL user account

To change the password of any of the user accounts that you have set up:

1. From the Start menu select:

   Websense Email Security > Database Tools > SQL User Management

   The **Websense Database Wizard Welcome** screen displays.
2. Select **Manage an MSDE/SQL Server User Account** and click **Next**. The **Manage an MSDE/SQL Server User Account** screen displays.
3. Select **Change Password for a SQL User Account** and click **Next**. The **MSDE/SQL Server Details** screen displays.
4. Select the server that contains the database.
5. Connect to the server using either:
   - A trusted connection
   - A username and password you supply
6. Click **Next**. The **Change password for a SQL User Account** screen displays.
7. Enter the user name, password and password confirmation and click **Next**.
8. A summary of your options displays.
   - If you need to change any details, click **Back**.
   - If the options are correct, click **Next**. A progress bar displays.

   A confirmation message displays when the Database wizard has changed the password.
9. Click **Finish**.

Deleting a SQL/MSDE account

To delete a SQL/MSDE user account:

1. From the **Start** menu select:

   Websense Email Security > Database Tools > SQL User Management

   The **SQL User Management** welcome screen displays.
2. Select **Manage an MSDE/SQL Server User Account** and click **Next**. The **Manage an MSDE/SQL Server User Account** screen displays.
3. Select **Delete a SQL user account** and click **Next**. The **MSDE/SQL Server Details** screen displays.
4. Select the server that contains the database.
5. Connect to the server using either:
   - A trusted connection
   - A username and password you supply
6. Click **Next**. The Delete a SQL User Account screen displays.
7. Enter the username and password of the account to delete and click **Next**.
8. A summary of your options displays.

- If you need to change any details, click **Back**.
- If the options are correct, click **Next**. A progress bar displays.

A confirmation screen displays when the account has been deleted successfully.

9. Click **Finish**.

Managing database authentication

Warning

You cannot set up SQL or NT authentication from a remote computer.

The Database Authentication settings control how Websense Email Security connects to the database. Websense Email Security can connect to the database using:

- SQL authentication
- NT authentication

Using SQL authentication

To use SQL authentication:

1. From the **Start** menu select:

   Websense Email Security > Database Tools > SQL User Management

   The **Websense Database Wizard Welcome** screen displays.
2. Select **Manage Database Authentication** and click **Next**. The **Manage Database Authentication Details** screen displays.
3. Select **SQL Authentication** and click **Next**. The **SQL Authentication Details** screen displays.
4. Enter the username and password of the account that Websense Email Security will use to connect to the database.
5. Click **Next**. A summary of your options displays.
   - If you need to change any details, click **Back**.
   - If the options are correct, click **Next**.

   A confirmation message displays when Websense Email Security has updated the authentication method.
6. Click **Finish**.

Using NT authentication

To use NT authentication:

1. From the **Start** menu select:

   Websense Email Security > Database Tools > SQL User Management

   The **Websense Database Wizard Welcome** screen displays.

2. Select **Manage Database Authentication** and click **Next**. The **Manage Database Authentication Details** screen displays.
3. Select **NT Authentication**.
4. Click **Next**. A summary of your options displays.
   - If you need to change any details, click **Back**.
   - If the options are correct, click **Next**.
5. A confirmation screen displays when the Database wizard has updated the authentication method.
6. Click **Finish**.

A Appendix A

Anti-Spam Agent - DFP Categories

The Anti-Spam Agent classifies spam into the following categories:

Overall category	Contains these categories
Core/Liability categories	• Adult • Gambling • Illegal material • Offensive • Phishing/fraud
Productivity categories	• Chain letters • Games/interactive • Novelty software • Computing/Internet • Health/medicine • Personal/dating • Entertainment • Products/services • Finance/home business • Humor • Special events • Other

For a detailed description of each category, see *Core/Liability categories*, page 282 and *Productivity categories*, page 283.

Core/Liability categories

The Core/Liability categories:

Category	Media Type	Definition
Adult	• Executable • Graphics • Movies • Sound • Text	• Adult humor, erotic stories, cartoons and animation or erotic chat • Adult products including sex toys, CD-ROMs and videos • Child pornography • Depictions or images of sexual acts, including sadism, bestiality or any form of fetish • Sexually exploitative or sexually violent text or graphics • Sexually oriented or erotic full or partial nudity
Gambling	• Executables • Text	• Online gambling or lottery sites that invite the use of real or virtual money • Virtual casinos • Fantasy sports leagues, sports picks and betting pools • Information or advice for placing wagers, participating in lotteries, or gambling, or running numbers
Illegal Material	• Executables • Graphics • Movies • Text	• Advice on performing illegal acts or obtaining illegal objects • Advocating, instructing, or giving advice on performing illegal acts such as phone service theft, evading law enforcement, lock-picking, fraud, plagiarism/cheating, and burglary techniques • Displaying, selling, or detailing the use of guns, weapons, ammunition or poisonous substances • Displaying, selling, or detailing use of drug paraphernalia • Hacking
Offensive	• Executables • Graphics • Movie • Sound • Text	• Promoting a political or social agenda that is supremacist in nature and exclusionary of others based on race, religion, nationality, gender, age, disability, or sexual orientation. For example, bigotry and racism. • Grotesque depictions • Offensive jokes and humor
Phishing/fraud	• Graphics • Movies • Sound • Text	• Virus hoaxes • Phishing scams • Deceptive or fraudulent information • Urban legends (for example, 419 scam and International Lottery scam)

Productivity categories

The Productivity categories:

Category	Media Type	Description
Chain Letters	• Executables • Text	• Mass email chain letters
Computing/ Internet	• Executables • Graphics • Movies • Sound • Text	• Spy software (spyware) • Hardware and software advertisements • Web hosting and Web design services • Questionnaires
Entertainment	• Graphic • Text·	• Entertainment and celebrity news • Promotions • Horoscopes, psychic readings and Chinese astrology • Hobbies and recreation
Finance /Home Business	• Executables • Graphics • Movies • Text	• Get-rich-quick schemes and multi-level marketing (MLM) • Debt consolidations and refinance schemes • Mortgage and loans promotional services • Stock quotes, stock tickers, and fund rates • Term life insurance • Work-at-home business reports & promotions
Games/Interactive	• Graphics • Text	• Online games and puzzles • Interactive quizzes, movies and programs
Health/Medicine	• Graphics • Text	• Prescription medicines promotions (for example, Viagra) • Weight loss, health supplements • Medical product promotions • Medical, dental and health insurance • Body modification and sexual enhancements
Humor	• Executables • Graphics • Movies	• Jokes and pranks (non-sexually explicit) • Humorous and satirical awards • Cartoons and humorous pictures
Novelty Software	• Text	• Cursor-changing software • Other software and gadgets intended for entertainment value rather than system performance
Personal /Dating	• Text	• Singles listings, matchmaking and dating services • Personal chat lines

Category	Media Type	Description
Products /Services	• Executables • Graphics • Movies • Text	• General product & service sales and advertisements • Promotions and commercials
Special Events	• Graphics • Movies • Sound • Text	• Festive and seasonal email, files, promotions • Email relating to a current event that may be objectionable, based on content, bandwidth, or negative impact on productivity such as a major sports event
Other	• Text	Items that do not fit into the other categories: • Job search • E-greeting cards and wishes • Questionnaires, polls and surveys • Stories, quotes, riddles, quizzes

B Appendix B

Supported file types

The table lists the file types that Websense Email Security can detect. The Dictionary Scanner and the File Attachment, Compress Attachments and Strip Attachments Rules objects can analyze a file in its native format even if its extension has been renamed. If a file type you want to detect is not listed here, you can add it to the file attachments object manually.

File Groups	File Types	Extensions
Archive Files	ARC compressed file archive	.arc, .pak
	ARJ compressed file	.arj
	BZIP compressed file	.bz, .bz2
	CAB compressed file	.cab
	GZIP compressed file	.gzip, .gz
	lbr compressed file	.lbr
	LZA self-extracting compressed file	.lza
	LHZ archive compressed file archive	.lha, .lzh
	Microsoft compressed archive	.cab
	RAR compressed file archive	.rar
	TAR archive file	.tar
	UNIX compressed file	.z
	UUE archive	.uue
	ZIP compressed file	.zip, .jar
	ZOO compressed file archive	.zoo

File Groups	File Types	Extensions
Audio Files	AIFF Audio file	.aif, .aiff
	CD Audio file	.cda
	MIDI Music file	.mid/.rmi/. midi
	MPEG Audio file	.mp3, .mp2, .mp1
	Ogg Vorbis Audio file	.ogg
	RealMedia file	.ra, .ram, .rm, .rmvb, .rts
	Sun/Next Audio file	.au
	Waveform audio file	.wav
	Windows ASF file	.asf
	Windows Media file	.wma
	Windows MIDI file	.mid

File Groups	File Types	Extensions
Data Files	dBASE (5.0 and earlier)	.dbf
	DataEase (4.x)	.dba, .dbm, .dql
	Data file	.dat
	First Choice (3.0 and earlier)	.pfc
	Font file	.fnt, .ttf
	Framework (3.0)	.fwk, .fw, .fw2, .fw3
	Information/setup file	.inf
	Microsoft Works (DOS) (?.? and earlier)	.wdb, .wks
	Microsoft Works (Mac) (?.? and earlier)	.wdb, .wks
	Microsoft Works (Windows) (4.0 and earlier)	.wdb, .wks, .dbf
	Open Office Database	.odb
	Paradox (DOS) (?.? and earlier)	.fsl, .db, .px
	Paradox (Windows) (?.? and earlier)	.fsl, .db, .px
	Personal R:BASE (1.0)	.rbf
	Program Information file	.pif
	Q & A	.qa, .qw, .dtf
	R:BASE 5000	.rbf, .dbf
	R:BASE System V (1.0)	.rbf
	Reflex (2.0)	.r2d
	SmartWare II (1.02)	.db, .def, .smt
	vCalender File	.vcs
	vCard File	.vcf
	Windows initialization file	.ini
	Windows registry file	.reg
	Windows shortcut	.lnk

File Groups	File Types	Extensions
Document Files	Adobe FrameMaker	.mif
	Adobe PDF	.pdf
	Compiled HTML Help file	.chm
	Corel/Novell Presentations (12.0 and earlier)	.shw, .cpr
	DCX tax file	.dcx
	DEC WPS Plus (WPL) (v4.1 and earlier)	.wpl
	DisplayWrite 2/3 (TXT)	.txt
	DisplayWrite 4/5 (2.0 and earlier)	.doc
	Enable document files (3.0, 4.0, 4.5)	.wpf
	Enable spreadsheet files (3.0, 4.0, 4.5)	.300, .wpf, .ssf, .dbf
	First Choice (3.0 and earlier)	.pfc
	Framework (3.0)	.fw3
	Freelance (Windows) (Millenium 9.6 and earlier)	.flw, .shw, .drw, .pre
	Freelance (OS/2) (2.0 and earlier)	.flw, .shw, .drw, .pre
	Hangul (97 and 2002)	.hwp
	Harvard Graphics (DOS) (2.x, 3.x)	.hgs, .cht, .ch3, .prs
	Harvard Graphics (Windows) (Windows versions)	.hgs, .cht, .ch3, .prs
	IBM FFT	.fft
	IBM Reversible Form Text	.rft
	IBM Writing Assistant (1.01)	.iwa
	Just System Ichitaro (4.x-6.x, 8.x-13.x, 2004)	.jaw, .jbw
	JustWrite (3.0)	.jw

File Groups	File Types	Extensions
Document Files (cont.)	Legacy (1.1 and earlier)	.leg
	Lotus 1-2-3 (DOS/ Windows) (5.0 and earlier)	.wku, .wk1, .wk2, .wk3, .wk4, .wk5, .wki, .wks
	Lotus 1-2-3 (OS/2) (2.0 and earlier)	.wku, .wk1, .wk2, .wk3, .wk4, .wk5, .wki, .wks
	Lotus 1-2-3 Charts (DOS/Windows) (5.0 and earlier)	.wku, .wk1, .wk2, .wk3, .wk4, .wk5, .wki, .wks
	Lotus 1-2-3 for SmartSuite (97 - Millenium 9.6)	.wku, .wk1, .wk2, .wk3, .wk4, .wk5, .wks, .123
	Lotus AMI/AMI Pro (3.1 and earlier)	.sam
	Lotus Manuscript (2.0)	.doc
	Lotus Symphony (1.0, 1.1, 2.0)	.wr1
	Lotus Word Pro	.lwp
	MacWorks document file	.wps
	MacWorks spreadsheet file	.wks
	MacWrite II (1.1)	.mcw, .mw, .mwii
	MASS11 (8.0 and earlier)	.m11
	Microsoft Access database	.mdb
	Microsoft Excel Charts (2.x - 7.0)	.xlc
	Microsoft Excel (DOS)	.xls
	Microsoft Excel (Mac) (3.0 - 4.0, 98, 2001, 2002, 2004, v.X)	.xls
	Microsoft Excel (Windows) (2.2 - 2003)	.xls, .xlw
	Microsoft Excel with password	.xls
	Microsoft Excel with VBA	.xlv
	Microsoft Multiplan (4.0)	.col, .cod, .mod
	Microsoft PowerPoint	.ppt

File Groups	File Types	Extensions
Document Files (cont.)	Microsoft Project	.mpp
	Microsoft Word (DOS) (6.0 and earlier)	.doc
	Microsoft Word (Mac) (4.0 - 2004)	.doc
	Microsoft Word (Windows) (2003 and earlier)	.doc
	Microsoft Word with password	.doc
	Microsoft Word with VBA	.doc
	Microsoft WordPad	
	Microsoft Works (DOS) (2.0 and earlier)	.wks, .wps, .wdb, .wcm
	Microsoft Works (Mac) (2.0 and earlier)	.wks, .wps, .wdb, .wcm
	Microsoft Works (Windows) (4.0 and earlier)	.wks, .wps
	Mosaic Twin (2.5)	.wku
	MultiMate (4.0 and earlier)	.dox
	Navy DIF	.dif
	Novell Perfect Works (2.0)	.wpw
	Office Writer (4.0 - 6.0)	.ow4
	OLE file	.ole
	Outlook message file	.msg
	PC-File Letter (5.0 and earlier)	.ltr
	PFS:Professional Plan (1.0)	.tid
	PFS:Write (A, B, C)	.pfb
	Professional Write (DOS) (2.1 and earlier)	.pw
	Professional Write Plus (Windows) (1.0)	.pw, .pwp
	Q&A (DOS) (2.0)	.qa, .qw, .dtf

File Groups	File Types	Extensions
Document Files (cont.)	Q&A Write (Windows) (3.0)	.dtf
	QuattroPro (DOS) (5.0 and earlier - text only)	.wkq, .wq1
	QuattroPro (Windows) (12.0 and earlier - text only)	.wb1, .wb2, .wk3
	Rich-text format document	.rtf
	Samna Word (IV+ and earlier)	.sam, .sm
	Signature (1.0)	.sig
	SmartWare II (1.02)	.def, .smt
	Sprint (1.0 and earlier)	.spr
	StarOffice/OpenOffice Calc (Windows and UNIX) (StarOffice 5.2 - 8.x; OpenOffice 1.1, 2.0 - text only)	.ods, .sdc
	StarOffice/OpenOffice Impress (Windows and UNIX) (StarOffice 5.2 - 8.x; OpenOffice 1.1, 2.0 - text only)	.sxd, .odp, .sxi, .sda, .sdd
	StarOffice Writer (5.2 - 8.x, text only)	.sdw, .sxw, .odt
	SuperCalc 5 (4.0)	.cal
	Websense Email Security message file	.msg
	Text file	.txt
	Total Word	.tw
	VolksWriter 3/4 (1.0 and earlier)	.vw
	VP Planner 3D (1.0)	.np
	Wang PC (IWP) (2.6 and earlier)	.iwp
	Windows Help file	.hlp
	Windows Write document	.wri
	WordMARC (Composer Plus and earlier)	.wmc

File Groups	File Types	Extensions
Document Files (cont.)	WordPerfect	.wpf
	WordPerfect (DOS) Versions through 6.1	.wpf
	WordPerfect (Mac) Versions 1.02 through 3.0	.wpf
	WordStar (DOS) (7.0 and earlier)	.ws
	WordStar (Windows) (1.0)	.ws
	WordStar 2000 (DOS) (3.0 and earlier)	.ws, .wst, .wsd
	XML document	.xml
	XyWrite (III Plus and earlier)	xy3, .xyp, .xyw

File Groups	File Types	Extensions
Drawing Files	3D studioMAX	.max
	Adobe FrameMaker Graphics Vector/raster (5.0 and earlier)	.fmv
	Adobe Illustrator (7.0, 9.0)	.ai
	Ami Draw	.sdw
	AutoCAD DWG file	.dwg
	AutoCAD DXF file	.dxf
	AutoShade Rendering (2.0)	.rnd
	Binary Group 3 Fax	.g3, .fax
	CALS Raster Type I and II	. gp4
	Computer Graphics Metafile (ANSI, CALS, NIST) (3.0)	.cgm
	GEM Paint	.img
	GEM bitmap and vector	.gem
	Hewlett Packard Graphics Language (2.0)	.hpgl
	IBM GDF (1.0)	.gdf
	IGES (5.1)	.iges
	JBIG2 graphics embedded in PDF files	.jbig
	Kodak Flash Pix	.fpx
	Kodak Photo CD (1.0)	.pcd
	Lotus PIC	.pic
	Lotus Snapshot	.snp
	Macintosh PICT1/ PICT2 (bitmap only)	.pict
	MacPaint	.pntg
	Micrografx Designer (3.1 and earlier)	.drw
	Micrografx Designer (Windows95) (6.0)	.dsf

File Groups	File Types	Extensions
Drawing Files (cont.)	Micrografx Draw (4.0 and earlier)	.drw
	Novell PerfectWorks (2.0)	.draw
	OS/2 PM Metafile (3.0)	.met
	Portable Bitmap	.pbm
	Portable Graymap	.pgm
	Portable Pixmap	.ppm
	Postscript (Levels 1-2)	.ps
	StarOffice/OpenOffice Draw file	.sxd, .sda, .odg
	Sun Raster	.srs
	Visio	.vsd, .vss, .vst, .vsw
	WBMP	.wbmp
	Windows Enhanced Metafile	.emf
	WordPerfect Graphics (2.0 and earlier)	.wpg, .wpg2
Email File Formats	Microsoft Outlook Folder	.pst
	Microsoft Outlook Message and Form template	.oft
	Microsoft Outlook Personal Address Book	.pab
	MIME Format Message File	.msg
Executable Files	Batch file	.bat, .cmd
	Executable file	.exe, .dll, .vxd, .sys, .cpl, .scr, .ocx, .oca, .com, .drv, .msi, .fon
	HTML Application	.htm, .html
	Java class file	.class
	JScript File	.js, .jse
	Netware loadable module	.nlm
	SHS scrap object	.shs, .shb
	VB Script file	.vbs, .vbe
	Windows script file	.wsf, .wsh

File Groups	File Types	Extensions
Image Files	Adobe PhotoShop	.psd, .pdd
	Adobe PostScript	.ps, .eps
	Bitmap	.bmp, .dib
	Corel Clipart (5 - 6)	.cmx
	Corel Draw file	.cdr
	Cursor file	.ani, .cur
	GIF	.gif
	IBM Picture Interchange Format (1.0)	.pif
	Icon file	.ico
	JFIF	.jpg, .jpe
	JPEG	.jpg, .jpeg, .jpe
	Paint Shop Pro	.psp
	PC Paintbrush Bitmap Graphic	.pcx, .dcx
	Portable Network Graphic (1.0)	.png
	Progressive JPEG	.jpg, .jpeg
	Targa version 2	.tga, .vda, .icb, .vst
	TIFF	.tif, .tiff
	TIFF CCITT Group 3/4 (6 and earlier)	.tif, .tiff
	Windows Metafile	.wmf
	X-Windows Bitmap (x10 compatible)	.xbm
	X-Windows Dump (x10 compatible)	.xwd
	X-Windows Pixmap (x10 compatible)	.xpm
Source Code Files	C/C++	.c, .cpp, .h, .hpp, .mak, .def, .idl, .rc, .rc2, .dsp; .dsw; .mdp
	Java	.java
	Perl	.pl
	Visual Basic	.vb, .bas, .frm, .frx, .vbp, .vbz

File Groups	File Types	Extensions
Video Files	Audio Video Interleave/ Video for Windows	.avi
	DVM movie	.dvm
	MPEG	.mpe, .mpeg, .mpg
	QuickTime	.qt, .mov
	ShockWave file	.swf
	Windows Media ASX file	.asx
Web Files	Cascading style sheet	.css
	ColdFusion file	.cfm
	HTML file	.htm, .html, .shtml, .asp, .php, .url
	Macromedia Flash file	.fla
	Single file Web page	.mht, .mhtml
	WML file	.wml
	Yahoo Instant Messenger	.ymg
File extensions	Encryption email formats	.p7c, .p7m, .p7s

Document decomposition

The following table details the types of documents that Websense Email Security can decompress using document decomposition.

Category of Format	Type	Version
Database	DataEase	4.x
	dBase	5.0 and earlier
	First Choice	3.0 and earlier
	FrameWork	3.0
	Microsoft Access	2.0 and earlier
	Microsoft Works (DOS)	2.0 and earlier
	Microsoft Works (Mac)	2.0 and earlier
	Microsoft Works (Windows)	4.0 and earlier
	Paradox (DOS)	4.0 and earlier
	Paradox (Windows)	4.0 and earlier
	Personal R:BASE	1.0
	Q&A	2.0 and earlier
	R:BASE 5000	3.1 and earlier
	R:BASE System V	1.0
	Reflex	2.0
	SmartWare II	1.02
Desktop Publishing	Adobe FrameMaker (MIF)	6.0
	Adobe PDF	2.1, 3.0-7.0
Email	Microsoft Mail Data	
	Microsoft Outlook Folder (.pst)	
	Microsoft Outlook Message and Form Template	97, 98, 2000, 2002, 2003
	Microsoft Outlook Personal Address Book (.pab)	
	MIME Format Message	
	Outlook Message	
Embedded Files	OLE	

Category of Format	Type	Version
Other	Executable (.exe, .dll)	
	Macromedia Flash	Flash, 6.x, 7.x, Lite (text only)
	Microsoft Project	98 - 2003
	MPEG Audio – ID3 information (meta data only)	
	vCalendar	2.1
	vCard	2.1
	WML	5.2
	XML (text only)	
	Yahoo Instant Messenger	6.x, 7.x
Presentation	Corel/Novell Presentations	12.0 and earlier
	Freelance (Windows)	Millenium 9.6 and earlier
	Freelance (OS/2)	2.0 and earlier
	Harvard Graphics (DOS)	2.x, 3.x
	Harvard Graphics (Windows)	Windows
	Microsoft PowerPoint (Windows)	3.0 - 2003
	Microsoft PowerPoint (Mac)	4.0 - v.X
	StarOffice/OpenOffice Impress (Windows and UNIX)	StarOffice 5.2 (text only), 6.x - 8.x (full support) OpenOffice 1.1, 2.0 (text only)

Category of Format	Type	Version
Spreadsheet	Enable	3.0, 4.0, 4.5
	First Choice	3.0 and earlier
	Lotus 1-2-3 (DOS and Windows)	5.0 and earlier
	Lotus 1-2-3 (OS/2)	2.0 and earlier
	Lotus 1-2-3 Charts (DOS and Windows)	5.0 and earlier
	Lotus 1-2-3 for SmartSuite	97 - Millenium 9.6
	Lotus Symphony	1.0, 1.1, 2.0
	Mac Works	2.0
	Microsoft Excel (Mac)	3.0 - 4.0, 98, 2001, 2002, 2004, v.X
	Microsoft Excel (Windows)	2.2 - 2003
	Microsoft Multiplan	4.0
	Microsoft Works (DOS)	2.0 and earlier
	Microsoft Works (Mac)	2.0 and earlier
	Microsoft Works (Windows)	4.0 and earlier
	Mosaic Twin	2.5
	PFS: Professional Plan	1.0
	QuattroPro (DOS)	5.0 and earlier (text only)
	QuattroPro (Windows)	12.0 and earlier (text only)
	StarOffice/OpenOffice Calc (Windows and UNIX)	StarOffice 5.2 - 8.x OpenOffice 1.1, 2.0 (text only)
	SuperCalc 5	4.0
	VP Planner 3D	1.0
Word Processing	DEC WPS Plus (DX)	3.1 and earlier
	DEC WPS Plus (WPL)	4.1 and earlier
	DisplayWrite 2 and 3 (TXT)	All
	DisplayWrite 4 and 5	2.0 and earlier
	Enable	3.0, 4.0 and 4.5
	Framework	3.0
	Hangul	97 and 2000
	IBM FFT	All
	IBM Revisable Form	All
	IBM Writing Assistant	1.01
	Just System Ichitaro	4.x - 6.x, 8.x - 13.x, 2004

Category of Format	Type	Version
Word Processing (cont.)	JustWrite	3.0 and earlier
	Legacy	1.1 and earlier
	Lotus AMI/AMI Professional	3.1 and earlier
	Lotus Manuscript	2.0 and earlier
	Lotus Word Pro (non-Windows)	SmartSuite 97, Millenium, Millenium 9.6 (text only)
	MacWrite II	1.1
	MASS11	8.0 and earlier
	Microsoft Word (DOS)	6.0 and earlier
	Microsoft Word (Mac)	4.0 - 2004
	Microsoft Word (Windows)	2003 and earlier
	Microsoft WordPad	All
	Microsoft Works (DOS)	2.0 and earlier
	Microsoft Works (Mac)	2.0 and earlier
	Microsoft Works (Windows)	4.0 and earlier
	MultiMate	4.0 and earlier
	Navy DIF	All
	Nota Bene	3.0
	Novell Perfect Works	2.0
	Novell/Corel WordPerfect (DOS)	6.1 and earlier
	Novell/Corel WordPerfect (Mac)	1.02 - 3.0
	Novell/Corel WordPerfect (Windows)	12.0
	Office Writer	4.0 - 6.0
	PC-File Letter	5.0 and earlier
	PFS:Write	A, B, C
	Professional Write (DOS)	2.1 and earlier
	Professional Write Plus (Windows)	1.0
	Q&A Write (Windows)	3.0
	Rich Text Format (RTF)	All
	Samna Word	4+ and earlier
	Signature	1.0
	SmartWare II	1.02

Category of Format	Type	Version
Word Processing (cont.)	Sprint	1.0
	StarOffice Writer	5.2 - 8.x (text only)
	Total Word	1.2
	Volkswriter 3 & 4	1.0 and earlier
	Wang PC (IWP)	2.6 and earlier
	WordMARC	Composer Plus and earlier
	WordStar (DOS)	7.0 and earlier
	WordStar (Windows)	1.0
	WordStar 2000 (DOS)	3.0 and earlier
	XyWrite	III Plus and earlier

C Appendix C

Anti-Virus return codes

The table lists the evaluation codes that the Anti-Virus Scanning object can return. When you include the Anti-Virus Scanning object in a rule, use these codes to specify what conditions will trigger the rule.

Return Code	Definition
0	No virus found
Virus found	
1	Virus found
3	Damaged file
5	Dangerous virus
6	Uncertified macros
7	Encrypted file
10	Virus found and repaired
11	Uncertified macros repaired
12	Auto-cured
15	Dangerous virus found and repaired
18	Boot virus found
19	Memory virus found
Anti-Virus 30-day evaluation period expired	
20	30-day evaluation period has expired
Virus Scanning Error	
21	Outdated virus data
22	Scan failed
23	Scan aborted
24	No DLL found
25	File not scanned

Return Code	Definition
26	File not found (file or disk access error)
27	No signatures
28	No interface
29	Incompatible version
30	Wrong thread
31	The queried interface is not supported
32	Initialization failure
33	Not initialized
34	The main body of virus data is missing
35	The virus data was corrupt
36	Some encryption error occurred. Probably a mismatch between NSE_xxx.LIB and NSE.DLL
37	Bad DLL format
38	I/O error during scan
39	Invalid parameter
40	Invalid structure
41	File is directory
42	File is protected
43	Access denied
44	Unexpected error
45	STRUCT.usSze not as expected by NSE
46	Error reading MCAFEE.MSG
47	Upgrade failed
48	Already initialized
49	Memory low
50	Cure failed
51	Cannot repair
52	Error during repair
53	McAfee: /FREQUENCY prevents scanner from proceeding
54	Cannot move virus pattern file

D Appendix D

Editing autoreply.txt

Autoreply.txt is a plain text file that contains messages for use with Rules Administrator objects and in the Message Administrator. Autoreply.txt contains messages you can use in notification and forwarded email in a range of circumstances. It is stored in the installation directory of Websense Email Security. You can edit it with a text editor, for example, Notepad. You can also remove the preset messages and replace them with new ones so long as the heading format remains the same.

Example messages in autoreply.txt:

[GENERAL]
<Your Company> filters all email automatically. This email contained non business related attachments or content and has been discarded. Please do NOT resend.
[END]

[VIRUS]
<Your Company> filters all email automatically. This email contained non-business related attachments or content that are suspected of having virus content. The event has been logged and message has been discarded. Please do NOT resend.
[END]

[GRTR4MB]
This is an automatic message. The files sent have been delayed until 9pm due to size > than 4MB. Contact postmaster@<Your Company>.com to send message immediately. Please ensure that any attachments are as small as possible prior to transmission. Files > 10MB will be discarded.
[END]

[OFFENSIVE]
This email contains material which could be deemed inappropriate and is isolated. It will be reviewed and discarded if found to be inappropriate.
[END]

[JOKES]
This email contains material which could be deemed inappropriate and has been isolated. It will be reviewed and discarded if found to be inappropriate.
[END]

[DEROGATORY]
This email contains material which could be deemed inappropriate and has been isolated. It will be reviewed and deleted if found to be inappropriate.
[END]

[GRAPHICS]
This email contains material which could be deemed inappropriate and has been isolated. It will be reviewed and discarded if found to be inappropriate.
[END]

[BLKMSITE]
This is an unsolicited email. Please remove the intended recipient from your email list.
[END]

Appendix E

Reporting using the STEMLog database

The diagrams that show the structure and relationships between the tables in the STEMLog database can be viewed by going to http://kb.websense.com and searching for “STEMLog database schema”. These relationships are used by Report Central to create reports on activity within Websense Email Security.

Index

D

E

R

S

T

U

V

W