TRITON - EMAIL SECURITY HELP

Websense® Email Security Gateway

v7.7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

R061277

Published June 2012
Printed in the United States of America and Ireland.

Trademarks

This product includes the following:

ANTLR

following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “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 COPYRIGHT OWNER 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 Apache Software License version 2

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.

dom4j

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “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 COPYRIGHT OWNER 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.

Bouncy Castle

Free Software Foundation, Inc.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

  a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

  b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

  c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply

to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Libevent

Copyright (c) 2000-2007 Niels Provos <provos@citi.umich.edu>. All rights reserved.

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. “

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “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 COPYRIGHT OWNER 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.

Net-SNMP

Copyright © 2001 - 2009 Net-SNMP. All rights reserved.

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “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 COPYRIGHT OWNER 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.

org.slf4j

Copyright (c) 2004-2008 QOS.ch All rights reserved.

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, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. 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. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Contents

1 Overview

Welcome to TRITON - Email Security, which provides maximum protection for email systems to prevent malicious threats from entering an organization's network. Email Security Gateway provides comprehensive on-premises email security hosted on a Websense® V-Series appliance (V10000 G2 and V5000 G2). Each message is scanned by a robust set of antivirus and antispam filters to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

A subscription to Websense Email Security Gateway Anywhere adds support for a hybrid service pre-filtering capability "in the cloud," which scans incoming email against a database of known spam. This feature can save network bandwidth and maintenance costs by dropping spam before it ever reaches an organization's network.

Integration with Websense Data Security provides valuable protection for an organization's most sensitive data.

Logging and reporting capabilities allow a company to view system status and generate reports of system and email traffic activity.

A Personal Email Manager facility allows authorized end users to manage email messages that Email Security policy has blocked but that may be safe to deliver. End users can maintain individual Always Block and Always Permit lists of email addresses to simplify message delivery.

Topics:

Administrator help overview

TRITON - Email Security Help includes the following topics:

Topic	Title	Description
1	Overview	Includes a brief introduction to TRITON - Email Security, administrator Help contents, and Websense Technical Support contact information
2	Getting Started	Provides an overview of the first-time Configuration Wizard, navigation descriptions and tips, dashboard customization, filtering database update information, and registration directions for the hybrid service and Data Security data loss prevention
3	Configuring System Settings	Includes details for configuring administrator roles, user directories, domain and IP address groups, appliance clusters, and system alerts, as well as Email Security management server backup and restore functions
4	Managing Messages	Contains information for setting message properties and directory harvest attack and relay control options, creating message routes and queues, and handling exceptions like encrypted messages
5	Working With Filters and Policies	Provides descriptions of filters, filter actions, policies, and global Always Block and Always Permit lists
6	Working With Reports	Includes an overview of reporting preference options, presentation report generation and management, and log database settings
7	Configuring End User Options for Personal Email Manager	Provides information about setting Personal Email Manager end-user options, including the contents of notification messages and whether an end user can manage personal block and permit lists; also contains details regarding end-user portal appearance and appliance deployment for managing a large volume of mail

Online help

Access online Help for Email Security Gateway from the **Help** button at the top right area of the screen, in the TRITON™ console module tray.

Click **Help > Explain This Page** to open context-sensitive help for the active Email Security Gateway screen.

> **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.)

Click **Help > Help Contents** to display the complete Email Security Gateway online Help. To find a Help topic in the Help viewer, select one of the following tabs:

- **Contents**

  Double-click a book icon to expand that book's topics.

  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 1 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.

Websense Technical Support

Click **Help > Support Portal** in the TRITON console module tray to access Websense online Support site. Technical information about Websense software and services is available 24 hours a day, including:

- the searchable Websense Knowledge Base (made up of a Solution Center and Technical Library)
- forums, Webinars, and show-me tutorials
- product documents and in-depth technical papers
- answers to frequently asked questions

For additional questions, click the **Contact Support** tab at the top of the page.

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.

For less urgent cases, use our online **Support Request Portal** at ask.websense.com.

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at MyWebsense.

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 the Websense management console
- Access to the machine running reporting tools and the database server (Microsoft SQL Server)
- Familiarity with your network's architecture, or access to a specialist

2 Getting Started

This chapter describes some basic Email Security Gateway configuration settings, some of which can be set in the first-time Configuration Wizard. Other topics covered include Email Security interface navigation, Today and History dashboard illustrations of Email Security system health and value, message and system logs, hybrid service and Data Security registration, and email filtering database update scheduling.

Topics:

Using the First-time Configuration Wizard

The Configuration Wizard is available the first time you open Email Security after installation. The wizard lets you quickly and easily enter some critical configuration settings before you open the TRITON - Email Security user interface.

Click the Email Security tab in the TRITON console module tray to display a pop-up box that allows you to enter your Email Security subscription key. You can enter your key here, or skip this step and enter your subscription key later in the **Settings** >

General > **Subscription** page (see *Entering and viewing subscription information*, page 7).

After you click **OK** in the subscription key pop-up box, a subsequent message box offers a choice of opening the Configuration Wizard or the Email Security Gateway dashboard.

> **Note**
>
> If you open the Email Security Gateway dashboard instead of the wizard, you are presented with an option to open a document containing some helpful configuration settings information.
>
> If you decide to skip the Configuration Wizard, you cannot access it later for this appliance.

You can enter the following information in the Email Security first-time Configuration Wizard:

- *Domain-based route*, page 6
- *Trusted IP addresses for inbound mail*, page 7
- *Email Security Log Server information*, page 7
- *Email Security system notification email address*, page 7

In order to save your settings, you must review them in the wizard's Confirmation page and click **Complete**.

Note that if you click **Cancel** at any time while you are in the Configuration Wizard, any settings you entered up to that point are lost.

A **Confirmation** page at the end of the wizard lets you review all your settings and modify any of them if desired. Click **Edit** next to the item you want to change to view the appropriate wizard page. Click **OK** on the edited page to return to the Confirmation page.

Click **Complete** when you are finished with your configuration settings. The Email Security Today dashboard opens.

Domain-based route

The **Domain-based Route** page of the Configuration Wizard lets you identify a domain that you want protected and designate the SMTP server to which mail to this domain should be sent. You can add more protected domains in the **Settings** > **Inbound/Outbound** > **Mail Routing** page.

Use the following steps in the wizard to designate a protected domain:

1. Enter a name for your route in the **Route name** entry field.
2. Designate a protected domain in the **Protected Domain Name** field.

3. Enter the SMTP server IP address and port number for the protected domain in the appropriate fields.
4. If you want email routing to use Transport Layer Security (TLS) to encrypt the transmission, mark the **Use Transport Layer Security** check box.
5. Mark the **Require Authentication** check box to force a user to enter username and password credentials. Enter the username and password that must be used.

Trusted IP addresses for inbound mail

In the Trusted Inbound Mail page, you can create a list of trusted IP addresses for which some inbound email filtering is not performed. Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

Enter an IP address in the **Trusted IP address** field, and then click the right arrow button to add it to the **Trusted IP address list**.

Delete an address from the Trusted IP addresses list by selecting the address and clicking **Remove**.

See *Managing domain and IP address groups*, page 50, for detailed information about how trusted IP addresses are handled in Email Security.

Email Security Log Server information

The Email Security Log Server receives records of system event and email filtering activity, which the Log Database uses to generate reports. Enter the Log Server IP address and port number on the **Log Server** page. Click **Check Status** to receive Log Server availability information.

Email Security system notification email address

You can identify an email address to which you want system notification messages sent in the **Notifications** wizard page. Typically, this is an administrator address. Enter the desired address in the **Notification email address** field.

Entering and viewing subscription information

You should receive an Email Security Gateway subscription key by email after you purchase the TRITON - Email Security module. If you did not enter the subscription key the first time you opened Email Security, enter it in the **Settings** > **General** > **Subscription** page.

After you enter a valid subscription key, the expiration date and number of subscribed users are displayed. Purchased subscription features appear in the Subscribed Features list.

Use the **Subscription key** field to enter a new key any time you receive one. If your subscription includes Websense Email Security Gateway Anywhere, you must register with the hybrid service every time you enter a new subscription key to establish the hybrid service connection.

Navigating TRITON - Email Security

The TRITON - Email Security user interface can be divided into 6 main areas:

- Banner
- Module tray
- Email Security Gateway toolbar
- Left navigation pane
- Right shortcut pane
- Content pane

The TRITON Unified Security Center banner shows:

- Your current logon account
- A Log Off button, for when you want to end your administrative session

The content displayed in TRITON - Email Security varies based on the privileges granted to the logged on user. A user who is a reporting administrator, for example, does not see server configuration settings or policy administration tools.

This section describes the options available to users with Super Administrator privileges.

The module tray lets you launch other modules of the TRITON Unified Security Center. For Websense Web Security or Data Security customers, click **Web Security** or **Data Security** to open the TRITON - Web Security or TRITON - Data Security module.

An Appliances button in the module tray opens a Manage Appliances window, which lets you add and remove an appliance in your system.

A TRITON Settings button lets you:

- Manage your administrator account.
- Add other TRITON administrators and assign them appropriate permissions.
- Specify and configure the desired directory service for TRITON administrators.
- Configure administrator account notification message details.
- Enable and configure two-factor authentication for administrator log on to the TRITON Console.
- Audit administrator logon attempts and changes to TRITON Settings.

See the TRITON Unified Security Center Help for more details.

The module tray also provides access to Explain This Page context-sensitive Help, complete Help system contents, helpful initial configuration setting information, and the Websense Support Portal.

The Email Security toolbar, just under the module tray, lets you switch between the Main and Settings tabs of the left navigation pane. Use the Main tab to access Email Security status, reporting, and policy management features and functions. Use the Settings tab to perform system administration tasks. The toolbar also includes a drop-down list of system appliances.

The right shortcut pane contains links to common administrative tasks. Click an item in the list to jump to the page where the task is performed.

Both the left and right navigation panes can be minimized by clicking the double arrow (<< or >>) icon at the top of the pane. Click the reverse icon (>> or <<) to view the pane. Click a shortcut icon on the minimized left navigation pane to access various groups of Email Security functions without maximizing the pane.

The Email Security Gateway Dashboard

The **Main > Status > Today: Health, Security and Value Since Midnight** page appears when you first log on to TRITON - Email Security. It displays alert messages and graphical charts that show the current state of your email scanning software, focusing on email traffic activity in your network. The charts on this page cover the 24-hour period beginning at 12:01 a.m. according to the time set on the Log Database machine.

At the top of the page, 2 summary sections provide a quick overview of current status:

- The **Health Alert Summary** shows the status of your Websense software. Click an error or warning alert message to open the Alerts page, where more detailed alert information is available (see *Viewing system alerts*, page 12).

  Information in the Health Alert Summary is updated every 30 seconds.
- Under **Business Value**, view statistics showing how Websense Email Security has protected your network today by blocking suspicious email traffic. Data includes total numbers and percentages of blocked messages listed by filter type, the percentages of false positive and negative results from spam scanning, and the number totals for various types of messages handled by Email Security.

Below the summary information, up to 4 user-designated Flash charts provide information about email scanning activities. These charts are available to Super Administrators, and to other administrators who are granted permission to view reports on the Today page. Click **Customize** to select the 4 charts you want displayed.

Information in these charts is updated every 2 minutes. You may need to scroll down to see all of the charts.

Up to 2 buttons appear at the top of the Today page:

- **Customize**, available to Super Administrators only, opens a page where you can select which charts to display on the Today page (see *Customizing the Today page*, page 10).
- **Print**, available to all administrators, opens a secondary window with a printer-friendly version of the charts on the Today page. Use browser options to print the page.

Related topics:

- *Customizing the Today page*, page 10
- *Customizing the History page*, page 11
- *Websense health alerts*, page 12
- *Viewing and searching logs*, page 14

Customizing the Today page

Use the **Today > Customize** page to select up to 4 charts for the **Status > Today** page. Only Super Administrators with unconditional policy permissions can customize the Today page. The following charts are available:

Chart Name
Connections Summary
Inbound Messages Summary
Outbound Messages Summary
Average Message Volume in Work Queue
Data Security Policy Violations by Severity
Top Data Security Policy Violations
Top Senders by Message Size
Top Senders by Message Volume
Top Blocked Protected Domain Addresses
Top Inbound Domains by Message Size
Top Inbound Domains by Message Volume
Top Recipients by Message Size
Top Recipients by Message Volume
Inbound Message Embedded URL Summary
Outbound Message Embedded URL Summary
Inbound Message Embedded URL Classification Summary
Outbound Message Embedded URL Classification Summary
Inbound Message Throughput

Chart Name
Outbound Message Throughput
Outbound Encrypted Messages Summary

Two additional reports are available if your subscription includes Websense Email Security Gateway Anywhere:

Chart Name
Hybrid Service Message Size Summary
Hybrid Service Message Volume Summary

The charts that you select appear on the Today page for all Super Administrators, and for other administrators who have permission to view charts on the Today page. See *Managing administrator accounts*, page 39.

Some charts show potentially sensitive information, such as usernames or IP addresses. Be sure that the charts you select are appropriate for all of the administrators who may view them.

To select charts, mark or clear the check box next to the chart name. When you are finished making selections, click **OK** to return to the Today page and view the charts. To return to the Today page without making changes, click **Cancel**.

Customizing the History page

Use the **Status** > **History: Last 30 Days** page to get an overview of email scanning activity for up to the past 30 days. The 4 charts on the page are updated daily at 12:01 a.m. to incorporate data from the previous day, as determined by the time on the Log Database machine. You may need to scroll down to see all the charts. See *Customizing the Today page*, page 10, for a list of available charts. Note that the Average Message Volume in Work Queue chart is not available for the History page.

The exact time period covered by the charts and summary tables depends on how long Email Security Gateway software has been processing mail. During the first month that Websense software is installed, the page shows data for the number of days since installation. After that, the reports cover the 30 days prior to today.

Depending on the reporting permissions granted to the role, some administrators may not see the charts on the History page. See *Managing administrator accounts*, page 39, for more information.

Two buttons appear at the top of the page:

- **Customize**, available to Super Administrators only, opens a page where you can change which charts appear on the page. You can also change the dollar amount used to calculate the estimated cost savings from the Email Security and hybrid service filtering capabilities.

- **Print**, available to all administrators, opens a secondary window with a printable version of the charts displayed on the History page. Use browser options to print this page, which omits all the navigation options found in the main TRITON - Email Security window.

Value Estimates

The Value Estimates section at the top of the History page provides an estimate of savings afforded by Email Security Gateway filtering capabilities, as well as a summary of blocked messages by email filter type.

Email Security filtering capabilities stop unwanted mail and threats, protecting network resources and saving an organization time and money. With the addition of the hybrid service (an Email Security Gateway Anywhere environment), infected traffic is stopped before it enters the network, increasing the savings.

Mouse over the Email Security Gateway Filtering Value item for an estimate of cost savings from hybrid service and Email Security email filtering. Default value of cost per MB includes the estimated cost saving from preventing threats and unwanted mail, and the resulting bandwidth saved. Click **Customize** in the **Estimated cost savings** pop-up box to set the cost savings per MB of blocked mail.

The Blocked area illustrates how Email Security software has protected your network. Total numbers and percentages of blocked messages are listed by filter type, including percentages of false positive and negative results from spam scanning.

Viewing system alerts

The **Health Alert Summary** on the dashboard shows the status of your Email Security software. Click an error or warning message to open the **Status > Alerts** page, where more detailed alert information is available.

The Alerts page displays information about problems affecting the health of your Email Security software, provides links to troubleshooting help, and documents the details of recent real-time filtering database updates.

The Active Alerts list shows the status of monitored Websense software components. For detailed information about which components are monitored, click **What is monitored?** above the list of alert messages.

To troubleshoot a problem, click **Solutions** next to an error or warning message. Click **Learn More** to find more details about an informational alert.

Websense health alerts

The Health Alert Summary lists any potential concerns encountered by monitored components of your Websense software. Alerts will be generated for the following conditions:

- Subscription expiration issues or subscription key problems
- Email Security services unavailable or not running

- Email Security configuration problems
- Master Database server connection problems
- Filtering database engine and download problems
- URL scanning server problems
- Log Server unavailable, not running, or having performance problems
- Email Security, Log Server, or Log Database version mismatches
- Log Database unavailable or having performance problems
- Presentation report jobs execution problems
- Low disk space problems
- Old system log or message queue files
- Unavailable system logs or message queues
- Third-party encryption application problems
- Appliance cluster connection and synchronization problems
- User directory server unavailable or not running
- Invalid user directory credentials

If you have subscribed to Websense Email Security Gateway Anywhere, or if your subscription includes both email and data security components, Websense software monitors interoperability components to provide alerts about the following conditions:

- Websense Data Security management server registration, configuration, and connection status
- Hybrid service registration, authentication, and connection status

The icon next to the alert message indicates the potential impact of the related condition.

The message is informational, and does not reflect a problem with your installation (for example, a successful database download or cluster synchronization).

The alert condition has the potential to cause a problem, but does not immediately prevent filtering or reporting (for example, hybrid service data is not available or the subscription key is about to expire).

A Websense software component is not functioning (has not been configured or is not running), which may impair filtering or reporting, or your subscription has expired.

Click an alert message in the Health Alerts Summary to go to the Alerts page, which provides additional information about current alert conditions. Click Learn More (for informational alerts) or Solutions (for errors or warnings) for details and troubleshooting tips.

Viewing and searching logs

Email Security Gateway includes 6 logs to help you monitor system and email message status. These logs are searchable by predefined time periods, or you can customize the time period you want searched. The Message Log also allows you to refine your search for messages, using search conditions like email address, scanning result, or message status.

You can export Message, Connection, or Hybrid Service log search results to a comma-separated value (CSV), HTML, or XML file. Other logs may be exported to a CSV or HTML file. Note that the maximum number of log entries exported cannot be greater than 100,000.

Email Security includes the following logs:

- *Message Log*, page 14
- *Connection Log*, page 18
- *Audit Log*, page 20
- *System Log*, page 22
- *Console Log*, page 23
- *Hybrid Service Log*, page 24

Message Log

The Message Log records information about each email message (inbound, outbound, and internal) processed by Email Security. Access the Message Log on the **Main** > **Status** > **Logs** page.

You can configure the number of entries per log page, between 25 and 200, in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Message Log pages by clicking the back and next arrows, or enter a specific page number in the **Page** field and click **Go**.

The length of time message records are saved in the database depends on your message volume and database partition capacity. To preserve message records, use the Export option to export the log on a regular basis. Exporting does not remove records from the Message Log. It transfers log data to a CSV, HTML, or XML file.

When the Message Log page appears, the most recent records are shown. Use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Message Log data

The following message data is collected and displayed in table format:

Message Data Item	Description
Message Log ID	A database-generated message identifier
Received Date/Time	The date and time a message was received
Subject	The message subject
Sender Address	Message sender email address
Sender IP	Message sender IP address
Recipient Address	Message recipient email address. If the message has multiple recipients, the first recipient address is displayed.
Scanning Result	Message filtering results (Clean, Virus, Spam, Data Usage, Exception, or Custom Content). When a Data Security policy is indicated, a **View Incident** link in this column opens the incident details in Data Security.
Message Status	Current message status (Delivered, Delayed, Dropped, Exception, or Failed). A message with multiple recipients may have multiple status entries based on the policy applied.

Message recipient details

When you click an individual message log identifier, details about that message are displayed. The following message detail items appear in table format:

Detail Item	Description
Recipient Address	Message recipient email address. If the message has multiple recipients, this column has multiple entries.
Recipient IP	Message recipient IP address
Direction	Message direction (Inbound, Outbound, or Internal). If the message has multiple recipients, this column may have multiple entries.
Delivered Date/Time	The date and time a message was delivered
Policy	Name of the policy applied to the message. If the message has multiple recipients, this column may have multiple entries.
Rule	Name of the policy rule applied to the message. If the message has multiple recipients, this column may have multiple entries for a single message. This item is blank for a message with a scanning result of Clean.
Scanning Result	Message filtering results (Clean, Virus, Spam, Data Usage, Exception, or Custom Content)

Detail Item	Description
Message Status	Current message status (Delivered, Delayed, Dropped, Exception, Failed)
Quarantined?	Indicator of whether message is quarantined (Yes or No). A **View Incident** link appears for a message isolated by a Data Security policy.

Message Log details

After you click a message in the Message Log ID column to view recipient details, a new **View Log Details** button is available at the bottom of the page. Message Log details appear in a table, with columns for the date and time of receipt, and the source of the message details. Detail sources can include message and connection control data, email policy data, and delivery data.

The log details appear in a third column, which can contain information about

- Message size, sender, and recipients
- Connection type, sender IP address, and the Email Security appliance that received the connection request
- Email policies and actions applied, including policy and rule names (filter and action), email direction (inbound, outbound, or internal), name of the virus or spam encountered, and the action taken as a result of filtering
- Hybrid service scanning results, including a DKIM validation, if applicable
- Message delivery dispositions, including recipient email and IP address, encryption type, and delivery status

Message Log search options

The Message Log includes several search options, including date range or keyword searches. Determine the date/time range for a search by selecting dates in the **View from/to** field calendar controls. Default value for the **from** or **to** field is the date and time that you open the log.

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list. Search for a keyword in all Message Log elements, or in 1 of the following Message Log components:

- Message Log ID
- Subject
- Sender Address
- Sender IP
- Recipient Address
- Scanning Result
- Message Status

Click **Set to Default** to return the keyword search options to the default settings (all Message Log components and keyword field blank).

View advanced search options for narrowing your message search by clicking **Advanced Options** to the right of the Keyword search box. Refine your search by selecting options in 1 or more of the following categories:

Category	Description
By Email Address	Click **Specify Email Addresses** to open the Specify Email Addresses dialog box. Specify your matching conditions, including email addresses; whether the address can be a sender, a recipient, or both; and whether the search should match any address in the list or all addresses in the list. The **Match Any** search option supports wildcard entries, but **Match All** does not. Separate email address entries by a semicolon (;).
By Scanning Result	Search by message filtering results (Clean, Virus, Spam, Data Usage, Custom Content, or Exception)
By Message Status	Search by current message status (Delivered, Delayed, Dropped, Exception, or Failed)

Click **Search** to generate search results.

Click **Set to Default** to return all your search option settings to their default state.

Message Log export options

To export Message Log search results:

1. Click **Export** to open the Export Log dialog box.
2. Select the desired output file type (CSV, HTML, or XML).
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
   - If you select **XML**, you can open the resulting file in Microsoft Excel.

     If Microsoft Excel is installed on the machine running TRITON - Email Security, the exported file opens. Use options in Excel to save or print the file. If Microsoft Excel is not installed on the machine running TRITON - Email Security, follow the on-screen instructions to either locate the software or save the file.
3. Indicate the pages you want to export (All, Current Page, or a page range).
4. Click **OK**.

Connection Log

The Connection Log is a record of incoming connection requests to Email Security and the results of connection scanning. Access the Connection Log on the **Main** > **Status** > **Logs** page by clicking the **Connection** tab.

You can configure the number of entries per log page, between 25 and 200, in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Connection Log pages by clicking the back and next arrows in the banner, or enter a specific page number in the **Page** field and click **Go**.

The length of time connection records are saved in the database depends on your connection volume and database partition capacity. To preserve connection records, use the Export option to export log data on a regular basis. Exporting does not remove records from the Connection Log. It copies log data to a CSV, HTML, or XML file.

When the Connection Log page appears, the most recent records are shown. Use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Connection Log data

The following connection data is collected and displayed in table format:

Connection Data Item	Description
Sender IP Address	The connection's sender IP address
Date/Time	The date and time a connection was received
Number of Messages	The number of messages in the connection

Connection Data Item	Description
Security Level	Encrypted or Not Encrypted
Connection Status	Current connection status (Accepted or Blocked). The reason for a blocked connection is displayed in an icon mouseover pop-up box in this column. Possible entries are as follows: • HELO/EHLO received before SMTP server greeting • Connection from <*server address*> failed SPF check. • Reverse DNS lookup failed. • Simultaneous connections from <*server address*> exceeded limit. • Message volume exceeded limits. • Message size exceeded limit. Message was forwarded to <*queue id*> queue. • File size exceeded limit. Message was forwarded to <*queue id*> queue. • Data size per connection exceeded limit. Message was forwarded to <*queue id*> queue. • HELO command syntax error • EHLO command syntax error • Percentage of invalid recipients exceeded limit. • Connection attempt by <*server name*> failed global Always Block list check. • Connection attempt by <*server name*> failed recipient validation check. • Connection attempt by <*server name*> failed user authentication. • Open relay from <*sender name*> blocked.

When you click an individual sender IP address link in the Connection Log, the Message Log opens and displays details about the message or messages associated with the selected connection. See *Message Log data*, page 15, for details.

Connection Log search options

The Connection Log includes several search options, including date range or keyword searches. Determine the date/time range for a search by selecting dates in the **View from/to** field calendar controls. Default value for the **from** or **to** field is the date and time that you open the log.

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list. Search for a keyword in all Connection Log elements, or in 1 of the following components:

- Sender IP address (wildcards and special characters are not supported in the keyword)
- Security Level
- Connection Status

Click **Search** to generate search results.

Click **Set to Default** to return the keyword search options to the default settings (**All** Connection Log components with the keyword field blank).

Connection Log export options

To export Connection Log search results:

1. Click **Export** to open the Export Log dialog box.
2. Select the desired output file type (CSV, HTML, or XML).
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
   - If you select **XML**, you can open the resulting file in Microsoft Excel.

     If Microsoft Excel is installed on the machine running TRITON - Email Security, the exported file opens. Use options in Excel to save or print the file. If Microsoft Excel is not installed on the machine running TRITON - Email Security, follow the on-screen instructions to either locate the software or save the file.
3. Indicate the pages you want to export (All, Current Page, or a page range).
4. Click **OK**.

Audit Log

Websense Email Security provides an audit trail showing which administrators have accessed TRITON - Email Security, as well as any changes made to policies and settings. This information is available only to Super Administrators. Monitoring administrator changes through the Audit Log enables you to ensure that system control is handled responsibly and in accordance with your organization's acceptable use policies.

Click the Audit Log tab on the **Main > Status > Logs** page to view the Audit Log, and to export selected portions of it to a CSV or an HTML file, if desired.

Audit records are saved for 30 days. To preserve audit records longer than 30 days, use the Export option to export the log on a regular basis. Exporting does not remove records from the Audit Log. It transfers log data to a CSV or HTML file.

When the Audit Log page opens, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the desired date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.

- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Below the View options, choose the number of log entries you want to view per log page from the **Per page** drop-down list (from 25 to 200). Default is 25. At the top and bottom of the page, scroll through the log using the back and next arrow buttons, or identify the page you want to see in the **Page** field and click **Go**.

Audit Log data

The log displays the following system audit information in table format:

Column	Description
Date	Date and time of the change, adjusted for time zones. To ensure consistent data in the Audit Log, be sure all machines running Websense components have their date and time settings synchronized.
User	Username of the administrator who made the change
Server	IP address of the appliance affected by the change
Client	IP address of the administrator machine that made the change
Role	Administrator role (Super Administrator, Auditor, Quarantine Administrator, or Reporting Administrator)
Type	The location of the change in the Email Security user interface (for example, if you enter a new subscription key, this column displays **General Settings | Subscription**)
Element	Identifier for the specific dynamic object changed, if any
Action	Type of change made (for example, add, delete, update, import, export, move, auth, sync, or reset)
Action Detail	A link that opens a Details message box with information about the change made

Audit Log export options

To export Audit Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, Last 7 days, or Last 30 days).

   Choose **Last 30 days** to export the entire Audit Log file.
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.

4. Click **OK**.

System Log

System Log records for Email Security Gateway reflect the current state of the system, along with any errors or warnings produced. Click the System Log tab on the **Main > Status > Logs** page to view the System Log, and to export selected portions of it to a CSV or HTML file, if desired.

System Log records are saved for 30 days. To preserve System Log records longer than 30 days, use the Export option to export the log on a regular basis. Exporting does not remove records from the System Log. It transfers log data to a CSV or HTML file.

When the System Log page opens, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the desired date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

You can also view log entries by type of system event by selecting an event type in the View by type drop-down list.

Below the View options, choose the number of log entries you want to view per log page from the **Per page** drop-down list (from 25 to 200). Default is 25. At the top and bottom of the page, scroll through the log using the back and next arrow buttons, or identify the page you want to see in the **Page** field and click **Go**.

System Log data

The log displays the following information:

Column	Description
Date	Date and time of the system event, adjusted for time zones. To ensure consistent data in the System Log, be sure all machines running Websense components have their date and time settings synchronized.
Server	IP address of the machine affected by the system event

Column	Description
Type	The type of system event (update, config exception, hybrid mode, cluster, log, quarantine, scan engine, DLP, patch and hotfix, watchdog, system maintenance, or alert)
Message	A link that opens a Details message box with information about the system event

System Log export options

To export System Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, Last 7 days, or Last 30 days).

   Choose **Last 30 days** to export the entire System Log file.
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
4. Click **OK**.

Console Log

The Console Log is a record of any administrator activities or changes made to the Email Security module of the TRITON Unified Security Center. Click the Console Log tab on the **Main > Status > Logs** page to view the Console Log, and to export selected portions of it to a CSV or HTML file, if desired.

The length of time Console Log records are saved in the database depends on your database partition capacity. To preserve Console Log records, use the Export option to export the log on a regular basis. Exporting does not remove records from the Console Log. It transfers log data to a CSV or HTML file.

When the Console Log page opens, the most recent records are shown. Use the **View** drop-down list options located above the log to select the range of log entries you want to see: All, One Day, One Week, One Month, or Custom. When you select **Custom**, use the **View from/to** fields to specify the desired date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Below the View options, choose the number of log entries you want to view per log page from the **Per page** drop-down list (from 25 to 200). Default is 25. At the top and bottom of the page, scroll through the log using the back and next arrow buttons, or identify the page you want to see in the **Page** field and click **Go**.

Console Log data

The log displays the following information:

Column	Description
Date	Date and time of the change, adjusted for time zones. To ensure consistent data in the Console Log, be sure all machines running Websense components have their date and time settings synchronized.
User	Username of the administrator who made the change
Client	IP address of administrator machine that made the change
Role	Administrator role that made the change, in this case, Super Administrator
Action	Type of change made (for example, Login, Logoff, Update user, Add device, Delete device, Log database change, Log server change, License change, or Switch device)
Action Detail	A link that opens a Details message box with information about the change made

Console Log export options

To export Console Log records:

1. Select a time period from the **Export range** drop-down list (Current page, Last 24 hours, Last 7 days, or Last 30 days).

   Choose **Last 30 days** to export the entire Console Log file.
2. Click **Go**.
3. Select the desired output file type in the **Export Log** dialog box.
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
4. Click **OK**.

Hybrid Service Log

The Hybrid Service Log contains records of email messages that are blocked by the hybrid service before they reach the network. You must have entered a valid subscription key for Email Security Gateway Anywhere and successfully registered Email Security with the hybrid service for the Hybrid Service Log to be available (see *Registering with the hybrid service*, page 28, for information).

After you register Email Security with the hybrid service, you can enable the Hybrid Service Log and set data delivery options on the **Settings > Hybrid Service > Hybrid Service Log Options** page. See *Configuring the Hybrid Service Log*, page 33, for information.

Access the Hybrid Service Log on the **Main > Status > Logs** page by clicking the Hybrid Service tab.

You can configure the number of entries per log page, between 25 and 200 (default is 25), in the **Per page** drop-down list in the log table banner. At the top and bottom of the page, scroll through Hybrid Service Log pages by clicking the back and next arrows, or enter a specific page number in the **Page** field and click **Go**.

The length of time message records are saved in the database depends on your message volume and database partition capacity. To preserve message records, use the Export option to export log contents on a regular basis. Exporting does not remove records from the Hybrid Service Log. It copies log data to a CSV, HTML, or XML file.

When the Hybrid Service Log page appears, the most recent records are shown. Use the **View from/to** fields to specify the date/time range for the log entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar.

Hybrid Service Log data

The following message data is collected and displayed in table format:

Message Data Item	Description
Hybrid Service Log ID	A database-generated message identifier
Date/Time	The date and time a message was received
Subject	The message subject
Sender Address	Message sender email address
Recipient Address	Message recipient email address. If the message has multiple recipients, the first recipient address is displayed.
Sender IP	Message sender IP address
Message Status	Current message status (e.g., discarded or bounced)
Reason	Supplied by the hybrid service, the scanning result that determines message disposition

Hybrid Service Log search options

The Hybrid Service Log has several search options, including date range or keyword searches. Determine the date/time range for a search by selecting dates in the **View from/to** field calendar controls. Default value for the **from** or **to** field is the date and time that you open the log.

You can perform a keyword search by selecting the log elements on which you want the search done from the **Keyword search** drop-down list and then entering a term in the field to the right of the list. Click **Search** to initiate the search function.

Search for a keyword in all Hybrid Service Log elements, or in 1 of the following Hybrid Service Log components:

- Hybrid Service Log ID
- Subject
- Sender Address
- Recipient Address
- Sender IP
- Message Status

Click **Set to Default** to return the keyword search options to the default settings (all Hybrid Service Log components and keyword field blank).

Hybrid Service Log export options

To export Hybrid Service Log search results:

1. Click **Export** to open the Export Log dialog box.
2. Select the desired output file type (CSV, HTML, or XML).
   - If you select **CSV**, a dialog box opens to let you open or save a text file in comma-separated value format.
   - If you select **HTML**, a dialog box opens to let you open or save an HTML file containing the log data.
   - If you select **XML**, you can open the resulting file in Microsoft Excel.

     If Microsoft Excel is installed on the machine running TRITON - Email Security, the exported file opens. Use options in Excel to save or print the file. If Microsoft Excel is not installed on the machine running TRITON - Email Security, follow the on-screen instructions to either locate the software or save the file.
3. Indicate the pages you want to export (All, Current Page, or a page range).
4. Click **OK**.

Security Information and Event Management (SIEM) integration

Third-party security information and event management (SIEM) tools allow the logging and analysis of internal alerts generated by network devices and software. Integration with SIEM technology lets Email Security Gateway transfer message activity events to a SIEM server for analysis and reporting.

Access SIEM integration settings on the **Settings > General > SIEM Integration** page. Mark the **Enable SIEM integration for all Email Security Gateway appliances** check box to activate SIEM integration functions.

After you enable SIEM integration, use the following steps to configure the SIEM server and transport protocol:

1. Enter the IP address or host name for the SIEM integration server in the **IP address or host name** entry field.
2. Enter the port number for the SIEM integration server in the **Port** field. Default is 514.
3. Select the protocol used for data transport, either **UDP** or **TCP**. User datagram protocol (UDP) is a transport layer protocol in the Internet protocol suite. UDP is stateless and therefore faster than transmission control protocol (TCP), but it can be unreliable. Like UDP, TCP is a transport layer protocol, but it provides reliable, ordered data delivery at the expense of transport speed.
4. Click **Send Test Message** to confirm that the SIEM product is properly configured and can receive messages from Email Security Gateway.

Hybrid service configuration

Websense Email Security Gateway Anywhere offers a flexible, comprehensive email security solution that lets you combine on-premises and hybrid (in-the-cloud) filtering as needed to manage inbound and outbound email for your organization.

The hybrid service provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

With Email Security Gateway Anywhere, you create policies for on-premises and hybrid filtering in the same user interface—TRITON - Email Security—and configuration, reporting, and management are centralized.

Before you can use the hybrid service to filter email for your organization, you must activate your hybrid account by entering a valid subscription key for Email Security Gateway Anywhere and configuring a number of settings in TRITON - Email Security and in your Domain Name System (DNS). This creates a connection between

the on-premises and hybrid portions of Email Security Gateway Anywhere. See *Registering with the hybrid service*, page 28, for details.

The Hybrid Service Log contains records of the email messages that are blocked by the hybrid service before they reach the network. See *Hybrid Service Log*, page 24, for information about the contents of this log. See *Configuring the Hybrid Service Log*, page 33, for details about enabling and scheduling Hybrid Service Log updates.

Registering with the hybrid service

Select **Settings** > **Hybrid Service** > **Hybrid Configuration** to activate your hybrid account. When you click **Register**, a registration wizard opens. Work through the pages in the wizard as follows:

1. *Enter customer information*, page 29
2. *Define delivery routes*, page 30
3. *Configure your DNS*, page 31
4. *Set up your firewall*, page 32
5. *Configure your MX records*, page 32
6. *Modifying hybrid service configuration*, page 33

Important

Multiple appliances controlled by a single Email Security Gateway management server share the same hybrid service configuration settings, regardless of appliance mode (cluster or standalone).

If you need to register more than 1 appliance with the hybrid service from the same Email Security management server, you should:

1. Add all your appliances to the Email Security Gateway management server (**Settings** > **General** > **Email Appliances**).
2. Create an appliance cluster, if desired (**Settings** > **General** > **Cluster Mode**).
3. Enter your Email Security Gateway Anywhere subscription key (**Settings** > **General** > **Subscription**).
4. Register with the hybrid service (**Settings** > **Hybrid Service** > **Hybrid Configuration**). If your appliances are operating in standalone mode, register from the appliance on which you entered the subscription key.

You may need to add an appliance after you have registered with the hybrid service (for example, after a new appliance purchase). In this situation, you should add the new appliance to the Email Security Gateway management server, then register your existing appliance with the hybrid service again without changing any configuration settings. Hybrid service configuration is synchronized across all appliances after you re-register.

Enter customer information

Use the Basic Information page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to provide the contact email address, phone number, and country for your Websense filtering administrators.

The email address is typically an alias monitored by the group responsible for managing your Websense software. This very important email sent to your account should be acted upon promptly when it is received.

- Websense Technical Support uses this address to send notifications about urgent issues affecting hybrid filtering.
- If there is a configuration problem with your account, failure to respond to an email message from Technical Support in a timely fashion could lead to service interruptions.

- Should certain rare problems occur, the email address is used to send information that allows Sync Service to resume contact with the hybrid service.
- This email address is **not** used to send marketing, sales, or other, general information.

The country you enter provides the system with time zone information.

Click **Next** to continue with hybrid configuration.

Define delivery routes

Use the Delivery Route page under **Settings > Hybrid Service > Hybrid Configuration** to define the domains for which email traffic will be routed to and from the hybrid service, and the SMTP server addresses that receive mail from and send mail to the hybrid service. Each group of one or more domains and one or more SMTP server addresses comprises a delivery route.

Important

Hybrid service checks the connection to your SMTP server by sending commands to a “postmaster” address. If your SMTP server does not have a postmaster or administrator address (e.g., postmaster@mydomain.com), you should add it manually before completing this step.

To add a delivery route:

1. On the Delivery Route page, click **Add**.
2. Enter a **Delivery route name**.
3. To add domains to your delivery route, click **Add** under Protected Domains.
4. Enter the **Domain Address** (for example, mydomain.com).
5. Define whether the delivery route should apply to all subdomains in the domain.
6. To add another domain, repeat steps 3 - 5.

Note

Protected domains added here must already be entered in the Protected Domain group on the **Settings > Users > Domain Groups** page. See *Managing domain and IP address groups*, page 50, for information.

7. To add inbound SMTP servers to your delivery route, click **Add** under SMTP Inbound Server Addresses.
8. Enter the IP address or name of your Email Security Gateway server. This must be the external IP address or name, visible from outside your network.

   To add more servers, click **Add** again. Each new server is given the next available ID number and added to the end of the list. The lowest ID number has the highest preference. Mail will always be received by the server with the highest

preference; if that server fails, the server with the next highest preference for that delivery route is used.

To change the preference order, check the box next to a server name, then click **Move up** or **Move down**.

9. To add outbound SMTP servers to your delivery route, click **Add** under SMTP Outbound Server Addresses. Email Security Gateway uses these IP addresses to send email to the hybrid service for encryption. See *Hybrid service encryption*, page 83, for information about this encryption function.
10. Enter the IP address or name of your Email Security Gateway server. This must be the external IP address or name, visible from outside your network.

    To add more servers, click **Add** again. Each new server is added to the end of the list. If an outbound server connection fails, email in this delivery route that needs to be encrypted is sent to a delayed messages queue for a later delivery attempt.
11. Click **OK**.

    The delivery route appears in the Route List on the Delivery Route page.

Click **Next** to continue with hybrid configuration.

Configure your DNS

Use the information on the CNAME Records page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to configure your DNS.

Before a delivery route is accepted by the hybrid service, it must first be checked to ensure that the service can deliver mail for each protected domain to your mail server and that each domain belongs to your company.

CNAME records are used to assign an alias to an existing host name in DNS. Contact your DNS manager (usually your Internet service provider) and ask them to set up a CNAME record for each of your protected domains, using the alias and associated domain information on the DNS page.

A CNAME record has the following format:

```
abcdefgh.mydomain.com CNAME autodomain.mailcontrol.com.
```

Where:

- `abcdefgh` is the **Alias** displayed on the DNS page
- `mydomain.com` is the **Protected Domain**
- `CNAME` indicates that you are specifying a CNAME record
- `autodomain.mailcontrol.com` is the **Associated domain** displayed with the above alias and protected domain

Make sure the trailing period is included in the associated domain name.

The above example indicates that the alias **abcdefgh.mydomain.com** is assigned to **autodomain.mailcontrol.com**. This enables the hybrid service to confirm that you own **mydomain.com**.

After you have created your CNAME records, click **Check Status** to verify that your entries are correctly set in your DNS. Resolve any error situations if necessary. If the **Check Status** button does not appear on the page, simply click **Next** to continue.

> **Note**
> The validation performed by clicking **Check Status** occurs in your local system. Because the propagation of DNS changes across all Internet servers can take between a few minutes to several hours, the verification process for the hybrid service may take longer.

Click **Next** to continue with hybrid configuration.

Set up your firewall

Use the information on the Network Access page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to configure your firewall.

Because the hybrid service is a managed service, Websense is responsible for managing system capacity. For this reason, the route of your email may occasionally alter within the hybrid service. To enable this to happen seamlessly without requiring you to make further changes, you must allow SMTP access requests from all the IP ranges listed on the Network Access page to Email Security Gateway port 25.

Click **Next** to continue with hybrid configuration.

Configure your MX records

Use the information on the MX Records page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to configure your Mail eXchange (MX) records.

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route inbound email through the hybrid service to Email Security Gateway.

Your MX records, which end in **in.mailcontrol.com**, are listed on the MX Records page. Contact your DNS manager (usually your Internet service provider) and ask them to set up or replace your current MX records for each protected domain you have specified with the customer-specific records provided by the hybrid service on the MX Records page. For example, they might change:

Change	From	To
MX Preference 1	mydomain.com. IN MX 50 mail.mydomain.com.	mydomain.com. IN MX 5 **cust0000-1.in.mailcontrol.com**.
MX Preference 2	mydomain.com. IN MX 51 mail.mydomain.com.	mydomain.com. IN MX 5 **cust0000-2.in.mailcontrol.com**.

Make sure they include the trailing period, and ask them to set each of these records to an equal preference value.

Check the entries on your Internet service provider's DNS management site to ensure they match the MX records provided by the hybrid service. After you validate your entries, click **Check Status** to verify that the update is successful.

It can take up to 24 hours to propagate changes to your MX records across the Internet. During this time, you should keep your previous mail routing active to ensure all your mail is delivered: while your MX records are changing over, some mail will be delivered using your old MX information, and some mail will be delivered using your new MX information.

Click **Finish** to complete your hybrid configuration.

Modifying hybrid service configuration

After you complete the registration wizard, you can review and modify your hybrid service configuration settings in the **Settings > Hybrid Service > Hybrid Configuration** edit page. .

> **Note**
> The **Check Status** button may not appear in the CNAME records area if the hybrid service has already verified domain ownership.

You should ensure that email is properly routed through the hybrid service by sending email to Email Security Gateway from outside your protected domains.

Configuring the Hybrid Service Log

Hybrid Service Log options are set on the **Settings > Hybrid Service > Hybrid Service Log Options** page. You can enable the Hybrid Service Log and determine the log's data transfer schedule on this page.

These options are available only if you have already entered a valid Email Security Gateway Anywhere subscription key and you have registered Email Security with the hybrid service.

Configure Hybrid Service Log options as follows:

1. Enable the Hybrid Service Log by marking the **Enable the Hybrid Service Log** check box.
2. Specify the time interval for retrieving the most recent Hybrid Service Log information in the **Retrieve Hybrid Service Log data every** drop-down box, from 15 minutes to 24 hours. Default is 15 minutes.
3. Specify the time interval for sending Hybrid Service Log information to the log database in the **Send the Hybrid Service Log data to the database every** drop-down box, from 15 minutes to 24 hours. Default is 15 minutes.
4. Click **OK**.

Registering with Websense Data Security

You can configure Email Security Gateway to scan your email for regulatory compliance and acceptable use and protect sensitive data loss via email by enabling the Data Security Email Data Loss Prevention policy in the **Main > Policy Management > Policies** page. Data Security policies are enabled by default. See *Enabling Data Security policies*, page 96, for more information about activating data loss prevention policies.

The Data Security Email Data Loss Prevention policy options are configured in the Data Security module of the TRITON Unified Security Center. See *TRITON – Data Security Help* for details.

You must register an Email Security Gateway appliance with the Data Security management server in order to take advantage of its acceptable use and data loss prevention features. Registration is automatic when you enter a valid Email Security Gateway subscription key. Subsequent appliances are registered when you add them to the TRITON Unified Security Center from the Email Security management interface.

If the Status field in the Email Security **Settings > General > Data Security** page displays **Unregistered**, you must register with Data Security manually.

Use the following steps in the Email Security **Settings > General > Data Security** page to register a standalone appliance with the Data Security management server:

1. Enter a valid Email Security Gateway subscription key in the **Settings > General > Subscription** page.
2. Specify the IP address used for communication with Email Security Gateway in the **Communication IP address** drop-down list.

   

   Note

   The appliance C interface IP address is selected by default. This setting is recommended for Data Security registration.

3. Select the **Manual** registration method to enable the Properties entry fields.
4. Specify the following Data Security server properties:
   - IP address
   - User name
   - Password
5. Click **Register**.

6. You must deploy Data Security policies in the Data Security module to complete the process. Click the Data Security module tab and then click **Deploy**.

> **Important**
> You should wait until Data Security policies are completely deployed before you register another standalone appliance.

The following issues apply if you are deploying Email Security Gateway in an appliance cluster:

- Register all the primary and secondary machines with Data Security before you deploy data loss prevention policies in Data Security. If you deploy Data Security policies on the primary appliance while you are registering a secondary machine with Data Security, the registration process for the secondary machine may not complete.
- Ensure that all machines in a cluster use the same physical appliance interface (the C, E1, or E2 IP address) to register with Data Security.

Email filtering database updates

Regular email filtering database updates offer maximum protection from email-borne attacks. Use the **Settings > General > Database Downloads** page to manage database updates for antispam and antivirus filters.

The Antivirus and Antispam filters tables list the set of filtering databases included in your Email Security subscription. If the current appliance is a primary machine, these tables also include update information for any secondary appliances associated with the primary appliance. A default update schedule of once every hour is included for each filter with your first database download.

To edit the update schedule for an individual filter, click **Edit** next to the database you want to change. In the Reschedule Filter Update dialog box, configure the following settings, as desired:

Frequency	How often you want the update to occur, from every 15 minutes to once every week
Day of week	This field is enabled only when the frequency selected is **Every week**. Choose the day of the week for the update.
Time	This field is enabled only when the frequency selected is **Every day** or **Every week**. Choose the time of day for the update.

Use **Update Now** to perform an immediate update of all antivirus or antispam databases.

URL scanning with Web Security

Email Security Gateway uses Websense Web Security URL scanning for accurate and efficient spam detection. The Web Security module maintains an updated URL master database from the Websense download server. Email Security Gateway queries the Websense URL category master database and determines the risk level of a URL found in an email message. Note that the Web Security version must be supported by Email Security Gateway for this function to be available.

Specify the location of the master database in the **Settings > General > URL Scanning** page:

- Use the **Local** option if Web Security and Email Security are installed on the same V-Series appliance.
- Use the **Remote** option to use a remote database. Enter the IP address or host name of the remote database.

Activate URL scanning in the **Main > Policy Management > Filters > Add URL Scanning Filter** page by marking the **URL scanning** check box in the Filter Properties section and selecting the URL categories for which you want Email Security to scan. See *URL Scanning*, page 90, for details.

Using a proxy server

You can configure a proxy server for email filtering database updates or for email traffic between the hybrid service and the Internet. Note that you can use the same proxy server for both functions.

Mark the **Enable filtering database update proxy server** check box if the proxy is used for database updates. Mark the **Enable hybrid service proxy server** check box if the proxy is used for hybrid service communication.

Note

Email Security Gateway does not support the use of a Secure Sockets Layer (SSL) proxy for filtering database updates. An SSL server may be used as a hybrid service proxy.

If you have Email Security Gateway and Websense Web Security Gateway running on the same Websense V-Series appliance (V10000 G2), Web Security Gateway can be set as the proxy server.

Use the **Settings > General > Proxy Server** page to enter proxy server information as follows:

1. Enter the IP address or host name of the proxy server in the **Server IP address or host name** field.

2. Enter the port number of the proxy server in the **Port** field.
3. Enter the username and password for the proxy server in the **Username** and **Password** fields.

Using the Common Tasks pane

The right shortcut Common Tasks pane provides shortcuts to frequently performed administrative tasks like running a report, creating a policy, or searching a log. Click an item in the list to jump to the page where the task is performed.

3 Configuring System Settings

This chapter describes other system configuration tasks to perform after you complete the Email Security Gateway first-time Configuration Wizard and enter some other initial settings. Topics covered include appliance management and cluster configuration, domain and IP address group configuration, user authentication setting, and user directory development. System alert specifications and backup and restore options for the Email Security management server configuration settings are also included.

Topics:

Managing administrator accounts

Email Security administrator accounts are created in the TRITON Unified Security Center Administrators page. Only a Super Administrator can add, edit, or delete an administrator account in the TRITON Settings page. Click **TRITON Settings** in the module tray to access the **TRITON Settings > Administrators** page.

A Super Administrator can create 2 types of accounts: local and network. A local account is stored in the local TRITON Unified Security Center database and contains a single user. A network account can contain a single user or a group of users and is stored on a network server. Details about managing TRITON console administrators on this page can be found in *TRITON Unified Security Center Help*.

An Email Security Super Administrator can also assign 1 of the following roles to a new administrator account on the Email Security Gateway **Settings** > **General** > **Administrator Accounts** page:

- Quarantine Administrator
- Reporting Administrator
- Auditor (the default role for a new Email Security specific account)

The Administrator Accounts page lists all defined Email Security administrators, their roles, and the administrator's current status (online or offline).

A user's view of the TRITON - Email Security management server interface is different, depending on that user's specific administrator role. For example, a user who is a Reporting Administrator can view only the items listed for the **Main** > **Status** left pane section of Email Security. An Auditor role means the user can view the entire Email Security management server interface, but that user cannot modify any settings. A user with a Quarantine Administrator role can search for, access, and manage blocked messages in assigned message queues, but cannot modify any Email Security settings.

By default, a new Email Security module-specific administrator account is an Auditor account. A Super Administrator can use the following steps to change an administrator's role:

1. Click **Edit Role** in the accounts table Role column on the **Settings** > **General** > **Administrator Accounts** page to open the Edit Role page.
2. In the Role Details box, make the desired changes to the administrator's role, selecting 1 of the following:
   - Auditor
   - Reporting Administrator
   - Quarantine Administrator
3. If you select **Quarantine Administrator**, you must specify at least 1 message queue that the administrator can access and manage. The message queues are listed by appliance name (primary and standalone machines only). All message queues are selected by default.
4. Mark the **Allow access to DLP incident queue** check box to allow a Quarantine Administrator to view Email Security Message Log **View Incident** entries (**Main** > **Status** > **Logs** > **Message Log**). Data Security incidents may also be viewed in the Blocked Messages queue (**Main** > **Message Management** > **Blocked Messages**). Viewing message details in the Data Security module requires permission from a Data Security Super Administrator. See *TRITON - Data Security Help* for details.
5. Click **OK**. Role changes are reflected on the Administrator Accounts page, along with the queues assigned to any Quarantine Administrator.

Only 1 Super Administrator may access an Email Security Gateway appliance at a time. Subsequent Super Administrators are assigned an Auditor (or read-only) role when they access the appliance.

Setting system preferences

You can accomplish the following Email Security system preferences on the **Settings** > **General** > **System Settings** page:

- *Entering the fully qualified domain name*
- *Setting the SMTP greeting message*
- *Setting system notification email addresses*
- *Configuring administrator console preferences*

Entering the fully qualified domain name

The SMTP protocol requires the use of fully qualified domain names for message transfer. Enter the appliance fully qualified domain name in the **Fully Qualified Domain Name** field (format is appliancehostname.parentdomain.com).

Important

This setting is important for proper Email Security Gateway operation. You must replace the default fully qualified domain name entry with the correct appliance name.

An incorrect fully qualified domain name may cause disruptions in email traffic flow.

Setting the SMTP greeting message

The SMTP greeting message is the response to a connection attempt by a remote server. It can also be used to indicate that the system is working properly. For example, the default SMTP greeting is

```
Websense Email Security Gateway Service is ready.
```

Change the default message by entering text in the **SMTP greeting** field.

Setting system notification email addresses

Email Security can automatically send notifications of system events like a stopped service to a predefined address, often an administrator address. Enter the desired recipient address in the **Administrator email address** field.

If you want notification messages sent to or from an administrator email address for other than system events, you must enter an address in this field as well. For example, configuring a notification to be sent to or from an administrator address when a message triggers a filter (in **Main** > **Policy Management** > **Actions**) requires that this field on the System Settings page contain an administrator address.

User notification messages may be sent from a predefined address. Enter the desired sender address in the **Default sender email address** field.

Configuring administrator console preferences

The Administrator Console Preferences section lets you configure your desired character set encoding and console language.

Select a character set for encoding messages from the **Preferred character encoding** drop-down list. The preferred character encoding setting is used to decode email attachments, including those for which no character encoding information is available.

Set the language you want the appliance to use in the **Administrator console language** drop-down list.

Managing appliances

Before you add an appliance to Email Security Gateway management, you should have already executed the V-Series appliance firstboot script to activate Email Security functions on the appliance and configured Email Security network interfaces in the V-Series Appliance Manager. Interface information includes IP address, subnet mask, default gateway, and up to 3 DNS server IP addresses. See Websense V-Series Appliance *Getting Started* for more details.

Note

The Appliance Manager allows you to configure a primary, secondary, and tertiary DNS server, with the secondary and tertiary servers being optional entries.

When it starts, Email Security Gateway polls each DNS server to determine which has the lowest latency level. That server is selected as the “primary” server for DNS queries, regardless of its designation in the Appliance Manager. The other servers may be used for subsequent queries based on the network connection status of the primary server.

If you change either the appliance host name or communication IP address on the appliance, you must make the same change in the Email Security **Settings > General > Email Appliances** page. Email Security does not detect this change automatically.

Email traffic is usually routed through dedicated appliance interfaces (E1/E2). However, if you want to route traffic through the C interface (for example, to transfer log data to a SIEM server), you need to define a route on the V-Series Appliance Manager **Configuration > Routing** page. You should note that you need to stop and restart Email Security Gateway services on the appliance each time you add or delete a route on the appliance.

Appliances overview

You can manage multiple Email Security appliances from the **Settings > General > Email Appliances** page without having to log on to each machine separately.Managed appliances share a single Log Database, from which Email Security log entries, presentation reports, and the Today and History pages dashboard statistics and charts are generated. The Email Security management server and all appliances must share the same version and subscription key for successful communication among the appliances.

An appliance may operate in standalone mode, which is the default mode when an appliance is added to Email Security management. You can also create appliance clusters by designating an appliance as a primary machine or as a secondary machine associated with a primary machine. See *Designating a primary appliance in a cluster*, page 45, for more information about appliance clusters.

The Email Appliances page lists all current system Email Security appliances in a table that shows the appliance host name, system communication IP address, system connection status, and mode. It also contains an Action column, with links that allow you to switch to a different appliance (**Launch**) that is in standalone mode or remove an unconnected primary appliance from a cluster (**Remove**). When a primary appliance is removed, all its secondary appliances change to standalone mode. The current appliance and all secondary appliances have an Action entry of **N/A**.

To add an Email Security appliance to the appliances list in the **Settings > General > Email Appliances** page:

1. Click **Add**.
2. In the Add Appliance dialog box, enter the IP address used for communication with the Email Security Gateway management server in the **System Communication IP Address** field.
3. Click **OK**.

Important

Changing the system communication IP address of an Email Security appliance in the V-Series Appliance Manager terminates the connection with Email Security Gateway. In order to re-establish the connection, the IP address must also be changed in the Email Security **Settings > General > Email Appliances** page.

You should also change the address for the Personal Email Manager notification message (**Settings > Personal Email > Notification Message**).

For Email Security Gateway Anywhere deployments, the hybrid service must be re-registered after you change the IP address.

When you add an appliance, it is automatically registered with the Data Security module for data loss prevention. To complete the registration process and deploy data

loss prevention policies, click Data Security on the TRITON toolbar and then click **Deploy**.

You can remove an appliance from the appliances list by selecting the appliance and clicking **Delete**. Note that you cannot delete an appliance that is being accessed by another user. Once you remove an appliance from the list, you cannot manage it from the Email Appliances page.

Editing appliance settings from the appliances list

You can edit the appliance communication IP address by clicking the appliance name in the appliances list. Note that the system connection status and mode cannot be changed on this page.

Configuring an appliance cluster

An Email Security Gateway appliance operates in standalone mode by default, but it can be configured in a cluster of appliances to manage a large volume of email traffic. After you have added an appliance to the appliances list on the Email Appliances page, you can change its mode from the default standalone to either primary or secondary in the **Settings > General > Cluster Mode** page.

Appliances in a cluster must all be of the same platform: all V10000 G2 or all V5000 G2, not a mix of the 2 platforms. Platform versions must also match in a cluster.

Deployed applications on appliances in a cluster must be the same. For example, all appliances in a cluster are Email Security only appliances, or they all have Websense Web Security in addition to Email Security.

Note

An appliance running Email Security Gateway and Web Security Gateway cannot be deployed in the same appliance cluster as an appliance running Email Security Gateway and Web Security.

Appliances in a cluster should also have the same message queue configurations. Messages in a secondary appliance queue may be lost if that queue is not configured on the primary machine before the cluster is created.

Important

If you are deploying Email Security Gateway in an appliance cluster and want to use Data Security policies, be sure to register all the primary and secondary cluster machines with Data Security before you deploy data loss prevention policies in Data Security.

If you deploy Data Security policies on the primary appliance while you are registering a secondary machine with Data Security, the registration process for the secondary machine may not complete.

Designating a primary appliance in a cluster

A primary appliance maintains and displays the configuration settings for all the appliances in its cluster. Use the following steps to specify a primary appliance in a cluster:

1. In the **Settings > General > Cluster Mode** page, select **Cluster (Primary)** as the appliance mode. A Cluster Properties box opens with the primary appliance IP address displayed in the **Cluster communication IP address** field. Secondary appliances use this IP address for cluster communications.

   

   Note

   Use of the C appliance interface IP address is recommended. If you use this interface, you need to define a route on the V-Series Appliance Manager **Configuration > Routing** page.

   You need to stop and restart Email Security Gateway services on the appliance each time you add or delete a route on the appliance.

2. Click **Add** to open the **Add Secondary Appliance** page, where you can designate the secondary appliances in this cluster.
3. Select the secondary appliances that you want to add to this cluster from the list of standalone appliances on the left (up to 7 appliances).

   If you want to add a new appliance that is not already on the list, click **Add New Appliance** to open the Add Appliance page.
4. Click the arrow button to add the appliances to the Secondary Appliances list.
5. Click **OK**. The appliance is added to the Secondary Appliances list along with its status.
6. Click **OK** in the main Cluster Mode page to complete the addition of the appliance to the cluster.

Click the appliance name in the Secondary Appliances list to open an Appliance Properties message box that contains all the details about the appliance.

You can remove a secondary appliance from a cluster by selecting the appliance in the Secondary Appliances list and clicking **Remove**.

Managing user directories

A user directory is an important component of email filtering, when it is used to set sender/recipient conditions for a policy. It can also provide recipient validation capabilities and be the basis of user logon authentication settings. You can add a user directory from the **Settings > Users > User Directories** page.

You can delete a user directory by selecting it in the user directories list and clicking **Delete**. You may delete a user directory only if Email Security is not using that directory. For example, if the directory is being used as part of a policy or as part of user authentication settings, it cannot be removed.

Adding and configuring a user directory

Click **Add** on the **Settings > Users > User Directories** page to open the Add User Directory page. After you name your user directory, select a user directory type from the drop-down list. Note that a new user directory has a status of **Not referenced**, because it is not yet being used by Email Security functions. User directory creation entries are different depending on the type of user directory you want.

Create a user directory by following the steps for the desired directory type:

- *Microsoft Active Directory*
- *IBM LDAP Server Directory*
- *Generic LDAP Server Directory*
- *Recipient List*
- *ESMTP Server Directory*

Microsoft Active Directory

Microsoft Active Directory provides user information management in a Windows environment. Use the following procedures to configure a Microsoft Active Directory in the User Directory Properties section:

1. Enter the IP address or host name of your LDAP server in the **Server IP address or host name** field.
2. Enter the port number in the **Port** field (default is 389).
3. Select the **Enable secure LDAP** check box if you want to enable secure LDAP, a nonstandard protocol also known as LDAP over SSL.

   Note that marking this check box changes the default port number to 636.

4. Enter the username and password for this appliance in the **Username** and **Password** fields. The Username field can contain the user's username, email address, or distinguished name.
5. Enter the LDAP server's search domain name in the **Search domain** field. This value is used when the search filter is applied.
6. The **Search filter** field should contain a standard LDAP query that can use validation variables like %user%, %domain%, and %email%.
7. Select either **Mirror** or **Cache address** as your cache setting.
   - The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking the **Synchronize** action for this directory on the User Directories page.
   - The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.
8. Enter a value in the cache timeout field. The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.
9. Mark the **Enable multiple user email account access in a single Personal Email Manager session** check box to activate this function for Personal Email Manager end users listed in this user directory.

IBM LDAP Server Directory

An IBM LDAP Server Directory provides user information management on an IBM server. Use the following procedures to configure an IBM LDAP Server Directory in the User Directory Properties section:

1. Enter the IP address or host name of your LDAP server in the **Server IP address or host name** field.
2. Enter the port number in the **Port** field (default is 389).
3. Select the **Enable secure LDAP** check box if you want to enable secure LDAP, a nonstandard protocol also known as LDAP over SSL.

   Note that marking this check box changes the default port number to 636.
4. Enter the username and password for this appliance in the **Username** and **Password** fields. The Username field can contain the user's username or distinguished name.
5. Select either **Mirror** or **Cache address** as your cache setting.

- The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking the **Synchronize** action for this directory on the User Directories page.
- The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.

6. Enter a value in the cache timeout field. The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.
7. Mark the **Enable multiple user email account access in a single Personal Email Manager session** check box to activate this function for Personal Email Manager end users listed in this user directory.

Generic LDAP Server Directory

A generic LDAP directory provides user information management that is supported on any LDAP server. Use the following procedures to configure a generic LDAP Server Directory in the User Directory Properties section:

1. Enter the IP address or host name of your LDAP server in the **Server IP address or host name** field.
2. Enter the port number in the **Port** field (default is 389).
3. Select the **Enable secure LDAP** check box if you want to enable secure LDAP, a nonstandard protocol also known as LDAP over SSL.

   Note that marking this check box changes the default port number to 636.
4. Enter the username and password for this appliance in the **Username** and **Password** fields. The Username field can contain the user's username or distinguished name.
5. Enter the LDAP server's search domain name in the **Search domain** field. This value is used when the search filter is applied.
6. The **Search filter** field should contain a standard LDAP query that can use validation variables like %user%, %domain%, and %email%.
7. Enter any optional email addresses to import in the **Mail field** text box.
8. Select either **Mirror** or **Cache address** as your cache setting.
   - The **Mirror** setting means that valid addresses are cached all at once by synchronizing the cache with all the addresses stored on the LDAP server. You can manually synchronize the cache with the LDAP server any time after that by clicking the **Synchronize** action for this directory on the User Directories page.

- The **Cache address** setting means the cache is updated dynamically. A new, valid address is cached after it is verified with the LDAP server. Remove all addresses from the cache by clicking **Clear cache**.

9. Enter a value in the cache timeout field. The timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.
10. Mark the **Enable multiple user email account access in a single Personal Email Manager session** check box to activate this function for Personal Email Manager end users listed in this user directory.

Recipient List

A recipient list is a text file that contains a list of email addresses and their associated passwords, 1 set per line. This file can be used for user recipient validation.

You can perform a keyword search on a recipient list by using the keyword entry field and Search button at the top of the Recipient List table. When your search results appear, a **View All** option allows you to view the entire recipient list.

Use the following procedures to configure a recipient list in the User Directory Properties section:

1. Add a predefined recipient list file by clicking **Browse** next to the **Recipient information file** entry field and navigating to the desired text file. The file format should be 1 email address and password per line, up to a maximum of 1000 entries.

   

   Note

   If you add a new recipient list file when you already have an active recipient list, the new file will overwrite the current file.

2. You can also create a recipient list by entering an individual email address and associated password in the **Enter Recipient Information** box and clicking the arrow button to add the information to the **Recipient List** box on the right.
3. Click **Search** if you want to perform a keyword search on your recipient list.
4. Click **OK**.

After you finish your recipient list entries, you can export the list to your local drive as a text file by clicking **Export**.

Remove an individual entry by selecting it in the **Recipient List** box and clicking **Delete**.

ESMTP Server Directory

An ESMTP Server Directory provides user authentication and recipient validation using the features in extended SMTP. Use the following procedures to configure an ESMTP Server Directory in the User Directory Properties section:

1. Determine your desired email verification method. Select **Use the return status of the VRFY command** to verify the email user name. Select **Use the return status of the RCPT command** to verify the email recipient.
2. Enter an email address for the user directory in the **Sender email address** field.
3. Enter a value in the cache timeout field. The cache timeout is the amount of time that a valid address remains in the memory cache. If an email message is sent from a previously validated address during this timeout period, the email is delivered without contacting the validation server. However, if another message is sent from this address after the timeout has expired, the server will be contacted to validate the address. Default value is 60 minutes.

   Remove all addresses from the cache by clicking **Clear cache**.

Managing domain and IP address groups

A collection of domain names or IP addresses can be defined in a single group for use in Email Security Gateway functions. For example, you can define a domain name group to establish domain-based delivery options, or you can define an IP address group for which Reputation Service, Real-time Blacklist (RBL), or directory attack prevention scans are not performed. IP address groups can also be used for the email encryption functions.

You can perform the following operations on domain or IP address groups:

- *Adding a domain group*
- *Editing a domain group*
- *Adding an IP address group*
- *Editing an IP address group*

You should note the following two special default groups of domain or IP addresses:

- Protected Domain group
- Trusted IP Address group

See *Third-party encryption application*, page 84, for information about using the Encryption Gateway default IP address group. Default groups cannot be deleted.

Protected Domain group

The Protected Domain group should contain all the domains that an organization owns and needs Email Security Gateway to protect. Message direction in Email Security is determined on the basis of an organization’s protected domains:

- Inbound - The sender address is not from a protected domain, and the recipient address is in a protected domain
- Outbound - The sender address is from a protected domain, and the recipient address is not in a protected domain
- Internal - Both the sender and recipient addresses are in a protected domain.

An open relay results when both the sender and recipient addresses are not in a protected domain.

Unless you entered a protected domain name in the Domain-based Route page of the First-time Configuration Wizard, the default Protected Domain group is empty after you install Email Security. Domains may be added to or deleted from the Protected Domain group, but you cannot delete the Protected Domain group itself.

Important

Ensure that the Protected Domain group contains all the domains you want Email Security to protect.

An open relay is created when mail from an unprotected domain is sent to an unprotected domain within your organization. As a result, Email Security may reject all mail from any domain that is not protected. Mail from an external trusted IP address to an unprotected domain within your organization bypasses analysis and is delivered.

The hybrid service uses the Protected Domain group during hybrid service registration to verify that the domains specified in its delivery routes are all from this group. The Protected Domain group should not be used to configure Email Security Gateway delivery routes (in the **Settings** > **Inbound/Outbound** > **Mail Routing** page) if you need to define domain-based delivery routes via multiple SMTP servers. See *Domain-based routes*, page 71, for information.

Trusted IP Address group

Like the Protected Domain group, the Trusted IP Addresses default group is empty after you install Email Security. IP addresses may be added to or deleted from the Trusted IP Addresses group, but you cannot delete the Trusted IP Addresses group itself. The Trusted IP Addresses group is limited to 32 addresses.

Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

Mail from an address in the Trusted IP Addresses group can bypass some inbound email filtering. Use of the Trusted IP Addresses group can result in improved email processing time.

Specifically, mail from trusted IP addresses bypasses the following email filtering:

- Global Always Block and Always Permit lists (**Main > Policy Management > Always Block/Permit**)
- All message controls except message size limitations (**Settings > Inbound/Outbound > Message Control**)
- Recipient validation (**Settings > Users > User Authentication**)
- All connection controls (**Settings > Inbound/Outbound > Connection Control**)
- Directory harvest attack (**Settings > Inbound/Outbound > Directory Attacks**)
- Relay controls (**Settings > Inbound/Outbound > Relay Control**)

> **Note**
> Mail from trusted IP addresses does not bypass policy and rule application, and it is always subject to antispam and antivirus filtering.

You may delete a domain or IP address group from its respective list by selecting the check box to the right of the name and clicking **Delete**.

Adding a domain group

Click **Add** on the **Settings > Users > Domain Groups** page to open the Add Domain Group page. Use the following procedures to add a domain group:

1. Enter a name for the new domain group in the **Domain Group Name** field.
2. Enter a brief description of your domain group.

In the Domain Group Details section, add a predefined domain group by clicking **Browse** next to the **Domain address file** field and navigating to the desired text file. The file format should be 1 domain address per line. If a file contains any invalid entries, Email Security accepts only the valid entries. Invalid entries are rejected.

1. You can also create a domain group by entering an individual domain address in the **Domain Address** field and clicking the arrow button to add the information to the **Added Domains** box on the right. Use wildcards to include subdomain entries (e.g., *.domain.com).
2. Click **OK**.

After you finish adding your domain address entries, you can export the list to your local drive as a text file by clicking the Added Domains **Export** button.

Remove an individual entry by selecting it in the **Added Domains** box and clicking **Delete**.

Editing a domain group

You can edit a domain group by clicking the domain group name in the **Settings > Users > Domain Groups** Domain Groups List to open the Edit Domain Group page. Add or remove individual domains on this page. You can also edit the domain group description.

Note that if a domain is in use, you will be asked to confirm any changes that involve that domain.

Adding an IP address group

Click **Add** on the **Settings > Inbound/Outbound > IP Groups** page to open the Add IP Address Group page. Use the following procedures to add an IP address group:

1. Enter a name for the new IP address group in the **IP Address Group Name** field.
2. Enter a brief description of your IP address group.
3. Add a predefined IP address group by clicking **Browse** next to the **IP address file** field and navigating to the desired text file. The file format should be 1 IP address per line.

   Note

   The default Encryption Gateway IP address group supports only the entry of individual IP addresses. Subnet address entries are considered invalid and are not accepted for this IP address group.

   Subnet addresses may be entered for other default and custom IP address groups.

4. You can also create an IP address group by entering an individual IP address in the **IP Address** box and clicking the arrow button to add the information to the **Added IP Addresses** box on the right.
5. Click **OK**.

After you finish adding your IP address entries, you can export the list to your local drive as a text file by clicking the Added IP Addresses **Export** button.

Remove an individual entry by selecting it in the **Added IP Addresses** box and clicking **Remove**.

Editing an IP address group

You can edit an IP address group by clicking the IP address group name in the IP Address Groups List to open the Edit IP Address Group page. Add or remove individual IP addresses on this page. You can also edit the IP address group description.

Note that if an IP address is in use, you will be asked to confirm any changes that involve that address.

Managing user validation/authentication options

After you define your domain groups, you can determine recipient validation and user authentication settings for users in the user directories you create. See *Managing domain and IP address groups*, page 50, for information about creating domain groups.

Three types of user validation/authentication are available in Email Security Gateway:

- **Recipient validation**, in which a message recipient is validated before a message is received
- **SMTP authentication**, in which a message sender is authenticated before a message is received
- **Personal Email authentication**, in which a user is authenticated before accessing the Personal Email Manager facility for managing blocked email. See *Configuring Personal Email Manager End User Options*, page 127, for details about the Personal Email Manager end-user tool.

Users in a domain group are verified against the corresponding user directory, and specified authentication settings are applied.

Important

You may create multiple Personal Email Manager user authentication groups. However, any protected domain group (as defined in **Settings > Users > Domain Groups**) may be included in only 1 Personal Email Manager user authentication group.

Including a protected domain group in more than 1 Personal Email Manager user authentication group may result in that domain group's users being denied access to the Personal Email Manager facility.

Be sure that you add all the user directories that contain the users in this protected domain group to the associated Personal Email Manager authentication group.

Click **Add** to create new recipient validation/authentication settings.

Click the name of existing authentication settings to modify the settings.

Remove a set of authentication settings by selecting it on the User Authentication page. Mark the check box next to the name of the settings. Click **Delete**.

Adding user authentication settings

Use the **Settings > Users > User Authentication** page to add new user validation/authentication settings for domain/user directory groups.

1. Click **Add** to open the Add User Authentication page.

2. Give this set of authentication settings a name.
3. Select the types of user validation/authentication settings that you want to apply.
4. Select the domain group you want to target with your authentication settings.

   You can add or remove domain names from your domain group by clicking **Edit** in the Domains area of the User Authentication page to open the Edit Domain Group page. Changes you make here are also reflected in the **Settings** > **Users** > **Domain Groups** page.
5. Select the corresponding user directories to which you want these authentication settings to apply by marking the check box next to the directory name and clicking the arrow button to add it to the Recipients box.

   Click **Add user directory** if you want to create a new user directory for these authentication settings. The Add User Directory page opens for you to create a new directory. See *Adding and configuring a user directory*, page 46, for user directory creation instructions.

   You can delete a user directory reference from the Recipients box by selecting it and clicking **Delete**. This action removes the user directory from the Recipients list, but does not delete it from the **Settings** > **Users** > **User Directories** page.

Editing user authentication settings

Edit existing authentication settings by clicking the name of the settings in the User Authentication page. Change any settings on the Edit User Authentication page. See *Adding user authentication settings*, page 54, for information about authentication settings.

Note that a user directory may be added or deleted from user validation/authentication settings. User directory entries are modified in the **Settings** > **Users** > **User Directories** page.

Managing Transport Layer Security (TLS) certificates

Transport Layer Security (TLS) is a protocol that provides an extra layer of security for email communications. Use of this protocol helps prevent devices such as non-trusted routers from allowing a third party to monitor or alter the communications between a server and client. Email Security can receive messages transferred over TLS and can also send messages via this protocol to particular domains.

A default TLS certificate is supplied with Email Security Gateway. After Email Security installation, default certificate information appears in the **Settings** > **Inbound/Outbound** > **TLS Certificate** page, in the Certificate Details section. Details include the certificate version, serial number, issuer, and expiration date.

You can generate a new certificate when that default one expires. On the **Settings** > **Inbound/Outbound** > **TLS Certificate** page, click **Generate** to create the new certificate. You should note that generating a new certificate overwrites any certificate that currently exists.

See the following sections for details on importing and exporting a certificate:

- *Importing a TLS certificate*, page 56
- *Exporting a TLS certificate*, page 56

Importing a TLS certificate

You may want to import a certificate rather than generate a new one in Email Security Gateway. You should note that importing a certificate overwrites any certificate that currently exists.

Import a certificate that is already located on your network as follows:

1. On the **Settings > Inbound/Outbound > TLS Certificate** page, click **Import**.
2. Click **Yes** in the confirmation dialog box. An Import Certificate area appears below the Import button.
3. Use **Browse** to navigate to the certificate file. When you select a file, its filename appears in the **Certificate file** field. File format must be .p12 or .pfx.
4. Enter a password in the **Password** field (maximum length is 100 characters).
5. Click **OK**.

Exporting a TLS certificate

If you want to export a TLS certificate and password to a location on your network, click **Export**. In the Save box, browse to the location where you want the certificate and password to be stored.

Backing up and restoring management server settings

The Email Security management server maintains several important configuration setting files, including

- Database configuration
- The Email Security Gateway appliances list
- The Email Security Gateway appliance groups list
- Email Security Gateway administrator settings
- Presentation report templates and data

You may want to retain a backup copy of these settings to use if a system recovery operation is necessary.

A backup and restore utility is installed, along with Email Security management features, on the management server.

The Backup/Restore function includes a Backup and Restore Log, which displays time-stamped backup and restore activities for the management server.

> **Note**
> Because the Backup/Restore utility stops the Email Security manager service, backup and restore activities are recorded only in the Backup and Restore log.

Backing up settings

The Email Security backup and restore functions are available on the **Settings > General > Backup/Restore** page. To back up your Email Security management server configuration settings, click **Backup** to activate the utility and specify a local folder for the backup file. That folder location appears in the File Location field in the Restore Settings section of the page.

If you want to save your backup settings on the Log Database server, mark the check box next to that option in the Backup Settings section. When you make this selection, the Remote Log Database Server Access box is enabled for you to enter server information. Indicate the domain name (if this field is not already populated with the remote log database host name), user name, password, and the backup/restore file path for the Log Database.

> **Note**
> The Email Security version of the backed up settings must match the version of the currently installed product.

Restoring the settings

Click **Restore** to use the Email Security backup/restore utility to return your settings to their original, backed up state on the Log Database server. The restore function retrieves the location of the backed up settings and applies them to the management server configuration files. Email Security restarts automatically after configuration settings are restored.

Configuring system alerts

In addition to displaying system alerts in the Today page dashboard Health Alert Summary, Email Security Gateway can use other methods to notify administrators that various system events have occurred. For example, notifications can be sent for updates to database download categories and subscription issues, as well as encryption and user directory issues.

Use the **Settings > Alerts > Enable Alerts** page to enable and configure the desired notification methods. Then, use the **Settings > Alerts > Alert Events** page to enable the types of alerts for which you want notifications sent.

Enabling system alerts

You can determine how alerts are distributed using 1 or more of the following delivery methods:

- To a specified individual via an email message
- To specified computers as a pop-up message
- To a specified community via an SNMP Trap system

Use the **Settings** > **Alerts** > **Enable Alerts** page to configure alert delivery methods.

When you are finished enabling alert methods, click **OK**.

Email alerts

Mark the **Enable email alerts** check box to have alerts and notifications delivered to administrators by email. Then, configure the following email settings:

Field	Description
From email address	Email address to use as the sender for email alerts
Administrator email address (To)	Email address of the primary recipient of email alerts
Email addresses for completed report notification	Email addresses for completed report notification recipients. Each address must be separated by a semicolon.

Pop-up alerts

Mark the **Enable pop-up alerts** check box to have alerts delivered via pop-up messages on specific computers. Then, enter the IP address or machine name for the desired computers, each entry separated by a semicolon.

SNMP alerts

Mark the **Enable SNMP alerts** check box to deliver alert messages through an SNMP Trap system installed in your network. Provide the following information about your SNMP Trap system:

Field	Description
Community name	Name of the trap community on your SNMP Trap server
Server IP or name	IP address or name of the SNMP Trap server
Port	Port number SNMP messages use

Alert events

To ensure that administrators are notified of system events, like a database download failure or a subscription that is about to expire, configure system alerts to be distributed by email, pop-up message, or through your SNMP Trap system.

Use the **Settings > Alerts > Enable Alerts** page to select the method used to send these alerts to Websense administrators.

Use the **Settings > Alerts > Alert Events** page to select the types of alerts to be delivered for each alert delivery method. Alerts are available for the following event types:

- Subscription expiration
- Email Security system events
- Log Server and Log Database events
- Mail queue events
- Email filtering events
- Encryption and decryption events
- Appliance cluster configuration events
- User directory server events
- Hybrid service operation events
- Signature update events
- SIEM server events
- Personal Email Manager server events

For each event type in the Alerts list, mark the delivery methods to be used. Marking the box in the column heading for each alert delivery method selects all the event types in that column. You must enable each other delivery method in the Enable Alerts page in order to select that method for an event type.

When you are finished, click **OK**.

4 Managing Messages

Email Security Gateway message handling is accomplished via a collection of configuration settings and message queue options. Message management settings in the **Settings > Inbound/Outbound** pages determine message size and volume limits, as well as which connections Email Security accepts and how many at a time. Prevent directory harvest attacks and open relays, and configure mail routes based on user directories or domain groups. Determine how to handle special situations like a message that is not deliverable or needs to be encrypted.

The **Main > Message Management** pages let you create and manage message queues for blocked and delayed email messages.

Topics

Configuring message properties

Email Security message control properties allow you to set message size and volume limits, and determine how invalid recipients are handled. Select **Settings > Inbound/Outbound > Message Control** to configure the following settings:

- *Enabling archive message options*, page 63
- *Enabling message sender verification*, page 63
- *Enabling bounce address tag validation (BATV)*, page 63
- *Enabling DomainKeys Identified Mail (DKIM) verification*, page 64

Click **OK** when you finish setting message properties.

Setting size properties

Use the Message Size Options to configure message size properties:

1. Select **Limit message size** (default setting) if you want to set a maximum message size.
2. Enter a maximum message size in the corresponding **Maximum message size (KB)** field, from 1 - 102400 (default is 10240). This setting can prevent very large messages from using valuable bandwidth.
3. Select **Limit data size per connection** if you want to set a maximum message size per connection.
4. Enter a maximum data size in the corresponding **Maximum data size (KB)** field, from 1 - 204800 (default is 20480). This setting can help limit the receipt of messages with very large attachments, which can take up valuable bandwidth.

Setting volume properties

Use the Message Volume Options to configure message volume properties:

1. Select **Limit number of messages per connection** to enable that option.
2. Enter a maximum number of messages per connection in the associated **Maximum number of messages** field, from 1 - 65535 (default is 30).
3. Select **Limit number of recipients per message** to enable that option.
4. Enter a maximum number of recipients in the corresponding **Maximum number of recipients** field, from 1 - 4096 (default is 20). This can save bandwidth by preventing one message from being sent to hundreds of users.

Configuring invalid recipient settings

Use the Invalid Recipient Options to configure invalid recipient settings:

1. Mark the **Allow invalid recipients** check box if you want to permit mail containing invalid recipients into your system. This option is available only when the recipient validation is used (see **Settings** > **Users** > **User Authentication)**.
2. Enter a value for the percentage of invalid recipients that determines if a message is blocked (default is 100).
3. Mark the appropriate check box to enable the system to send a non-delivery receipt (NDR) notification only if a message is not blocked.

Enabling archive message options

Mark the **Enable archive queue storage** check box if you want all incoming messages saved to an archive message queue before they are scanned. You should note that enabling this feature can impact storage capacity and system performance. This option is disabled by default.

View the archive queue by clicking **archive** in the queue list on the **Main** > **Message Management** > **Message Queues** page.

Enabling message sender verification

Ensure that an internal email sender is an authenticated user by enabling the internal sender verification function. This operation performs a check to confirm that an email sender from an internal domain is also an authenticated user. For email to pass this check function, a mail sender's address must match the sender's log in authentication entry.

Mark the **Enable internal sender verification** check box in the Internal Sender Verification section to activate this function. By default, this function is disabled.

Enabling bounce address tag validation (BATV)

Bounce address tag validation (BATV) is a method for determining whether a bounce message to an address in your protected domain is valid. This method helps to prevent backscatter spam, in which a bounce message to your organization contains a forged recipient address.

With BATV enabled, Email Security Gateway marks the sender address of outbound email with a unique tag. A bounce message addressed to that sender is examined for the presence of that unique tag. If Email Security detects the tag, the bounce message is cleared for delivery. A bounce message without the tag is blocked.

Enable BATV in the **Settings** > **Inbound/Outbound** > **Message Control** page. Mark the **Enable Bounce Address Tag Validation** check box in the Bounce Address Tag Validation section.

You may want mail from some user and IP address groups to bypass the BATV function. These groups can be defined in the Bounce Address Tag Validation section. Select a group from among the following drop-down lists:

- Inbound IP address group
- Inbound domain group
- Outbound domain group

Note that a domain group selected for outbound bypass must also be selected for inbound bypass.

The default setting for each group is **None**. Only user-defined domain and IP address groups are available in the drop-down lists. See *Managing domain and IP address groups*, page 50, for information about creating domain and IP address groups.

Enabling DomainKeys Identified Mail (DKIM) verification

DomainKeys Identified Mail (DKIM) is a validation method that uses a message header digital signature to associate a domain name with the email. Email Security Gateway has a DKIM signature verification function that can retrieve signer information, including a public key, from the DNS. Email Security analyzes and verifies the signer information to determine message legitimacy.

You can enable Email Security Gateway DKIM verification in the **Settings > Inbound/Outbound > Message Control** page, in the DomainKeys Identified Mail (DKIM) Verification section. Mark any of the following check boxes to activate DKIM verification:

- **Enable DomainKeys Identified Mail (DKIM) verification for inbound messages**
- **Enable DomainKeys Identified Mail (DKIM) verification for outbound messages**
- **Enable DomainKeys Identified Mail (DKIM) verification for internal messages**

By default, these check boxes are not marked.

You can configure a custom content policy filter to scan for a DKIM signature in the message header, along with a filter action to take when a message header triggers the filter. See *Custom Content*, page 88, for information about creating this filter.

Managing connection options

You can improve system performance by limiting the number of simultaneous connections made to Email Security Gateway. In the **Settings > Inbound/Outbound > Connection Control** page, Connection Options section, enter the maximum number of allowed simultaneous connections per IP address, from 1 - 10000 (default is 10). Specify the maximum number of seconds of inactivity allowed before a connection is dropped, from 1 - 43200 (default is 300).

You can also configure the following settings in the Connection Control page:

- *Using a real-time blacklist (RBL)*, page 65
- *Using reverse DNS verification*, page 65
- *Using Websense reputation service*, page 65
- *Delaying the SMTP greeting*, page 66
- *Enabling the SMTP VRFY command*, page 66
- *Using access lists*, page 66

Click **OK** when you finish configuring connection control settings.

Using a real-time blacklist (RBL)

A Real-Time Blacklist (RBL) is a third-party published list of IP addresses that are known sources of spam. When RBL checking is enabled, messages from a sender listed on an RBL are prevented from entering your system.

In the Real-time Blacklist (RBL) Options section, mark the **Perform RBL check** box to enable RBL checking. Enter the domain addresses of up to 3 third-party RBLs you want to use in the **Domain address** field. Separate multiple addresses with a semicolon (;).

This feature is not enabled by default.

Using reverse DNS verification

Reverse DNS lookup uses a pointer (PTR) record to determine the domain name that is associated with an individual sender IP address. With reverse DNS lookup, Email Security ensures that email sent to your system is from a legitimate domain.

Note that if you enable Reverse DNS, server performance may be affected, or legitimate users may be rejected. This function is not enabled by default.

You can determine the Email Security response to a reverse DNS lookup by selecting 1 or more of the following options in the Reverse DNS Lookup Options section:

- **Disconnect if the PTR record does not exist.**
- **Disconnect if the PTR record does not match the A record.**
- **Disconnect if a soft failure occurs during a reverse DNS lookup.**
- **Disconnect if the PTR record does not match the SMTP EHLO/HELO greeting.**

Using Websense reputation service

Email Security Gateway can check an email sender's IP address against the Websense reputation service, which classifies email senders based on past behavior. With this function, Email Security can block mail from known spam senders.

To use the Websense reputation service, mark the **Enable Reputation Service** check box (the default setting) in the Reputation Service Options section. Then select 1 of the following scanning levels to specify the threshold for blocking mail:

- **Conservative**, which blocks mail from addresses that send spam 100% of the time
- **Medium**, which blocks mail from addresses that send spam 99% of the time
- **Aggressive**, which blocks mail from addresses that send spam 97% of the time

Delaying the SMTP greeting

You can specify that an SMTP greeting message be delayed for a specified time interval, so that a connection from a client will be dropped if the client tries to send data during this time interval. This option can help prevent mail from spam-sending applications that send a high volume of messages very quickly. The connection is dropped as soon as a message is sent to the SMTP server before it is ready.

Enable the SMTP greeting delay by marking the **Enable SMTP greeting delay** check box in the SMTP Greeting Delay Options section. Specify the delay time, in seconds, from 1 - 60 (default is 3).

This feature is not enabled by default.

Enabling the SMTP VRFY command

The SMTP VRFY command can be used to verify an email username. When asked to validate a username, a receiving mail server responds with the user's login name. Enable this command by marking the **Enable SMTP VRFY command** check box (the default setting) on the **Settings > Inbound/Outbound > Connection Control** page in the SMTP VRFY Command Option section.

Important

Use this command with care. Although helpful in validating a user, this command can also create a network security issue if the user information is retrieved by someone with malicious intent.

Using access lists

An access list enables you to specify an IP address group for which certain email scanning is not performed. The Allow Access List Options in the **Settings > Inbound/Outbound > Connection Control** page let you identify these IP addresses. Mail from these addresses bypasses the following email filter scanning:

- Connections per IP address
- RBL checks
- Reverse DNS lookup
- Reputation service
- SMTP greeting delay
- Directory harvest attack prevention
- Inbound relay control

Because mail from the Trusted IP Address group bypasses additional email filtering, that group should not be entered in the Allow Access List. See *Managing domain and IP address groups*, page 50, for details.

You define IP address groups in **Settings > Inbound/Outbound > IP Groups**. The groups you have defined on that page appear in the Connection Control Allow Access List Options section, in the **IP group** drop-down list.

To create and modify an access list:

1. Select an IP group name in the **IP group** drop-down to display the addresses in the **IP addresses** list and enable the **Edit** button.
2. Click **Edit** to modify the access list in the Edit IP Groups page.
3. Add a predefined IP address group by clicking **Browse** next to the **IP address file** field and navigating to the desired text file. The file format should be 1 IP address per line.
4. You can also enter an individual IP address in the **IP Address** box and click the arrow button to add the information to the **Added IP Addresses** box on the right.

> **Note**
> Any changes made here to an IP address group are reflected in the **Settings > Inbound/Outbound > IP Groups** page.

5. Click **OK**.

When you have finished your access list, you can export the list to a location in your network. Click **Export** to save the access list file to another location.

You can delete an IP address from the Added IP Addresses list by selecting it and clicking **Remove**.

Controlling directory harvest attacks

A directory harvest attack is used by questionable sources to gain access to an organization's internal email accounts. A directory attack not only consumes large amounts of system resource but also, through the acquisition of email accounts, creates spam problems for email end users. With directory attack prevention settings, you can limit the maximum number of messages and connections coming from an IP address over a given time period.

To configure directory attack control:

1. Select **Settings > Inbound/Outbound > Directory Attacks**.
2. Select the **Limit the number of messages/connections per IP every** check box to enable the directory harvest attack prevention function.
3. Set the time period, from 1 second to 60 minutes, in the drop-down list (default is 60 seconds).
4. Set the maximum number of messages allowed from an individual IP address during the specified time period (default is 30).

5. Set the maximum number of connections allowed from an individual IP address during the specified time period (default is 30).
6. If you have enabled the directory attack prevention option, you can also enable settings to block an IP address when a specific set of recipient conditions occurs. Mark the **Block the IP address for** check box, and enter the time interval during which you want an IP address blocked (default is 3 hours).
7. Enter the conditions for blocking the IP address:
   - Maximum number of message recipients (default is 5)
   - Maximum percentage of invalid addresses among the recipients (default is 50%)

   When these recipient limitations are exceeded, the connection is dropped automatically.

   This option is available only when the recipient validation option is used (see *Adding user authentication settings*, page 54).

Configuring relay control options

You can prevent the unauthorized use of your mail system as an open relay by limiting the domains and IP address groups for which your server is allowed to relay mail. Protected domains are defined in the **Settings > Users > Domain Groups** page. Trusted IP address groups are defined in the **Settings > Inbound/Outbound > IP Groups** page.

Configure relay control settings in the **Settings > Inbound/Outbound > Relay Control** page as follows:

1. In the Inbound Relay Options section, set any desired option that is based on the Sender Policy Framework (SPF) of the sender domain:
   - **Reject mail if no SPF record exists.**
   - **Reject mail if the SPF record does not match the sender's domain and a soft fail occurs.**
   - **Reject mail if an SPF error occurs.**

   By default, these options are not enabled.
2. In the Outbound Relay Options section, select the relay setting for senders in protected domains when SMTP authentication is not required. Default setting is **Allow relays only for senders from trusted IP addresses**.

   Note that allowing all outbound relays may create a security vulnerability in your system.
3. In the Internal Relay Options section, select the relay setting for mail between protected domains when SMTP authentication is not required. Default setting is **Allow relays only for senders from trusted IP addresses**.

   Note that allowing all outbound relays may create a security vulnerability in your system.

Configuring delivery routes

Configure delivery routes in the **Settings** > **Inbound/Outbound** > **Mail Routing** page. You can create the following types of message routes:

- *User directory-based routes*, page 69
- *Domain-based routes*, page 71

Change the order of a user directory- or domain-based route by marking its associated check box and using the **Move Up** or **Move Down** buttons.

Copying a route

Use the following steps to copy a route in the **Settings** > **Inbound/Outbound** > **Mail Routing** page:

1. Select a route in the route list by marking the check box next to its name.
2. Click **Copy**. A new route appears in the route list, using the original route name followed by a number in parentheses. The number added indicates the order that copies of the original route are created (1, 2, 3, etc.).
3. Click the new route name to edit route properties as desired.

Removing a route

If you want to remove a route, select the route by marking the check box next to its name and click **Delete**.

Note that the default domain-based route cannot be deleted.

User directory-based routes

Delivery routes based on user directory entries are scanned first for a match with an email message recipient. Domain group entries are validated against the selected user directory to determine whether email will be delivered via a specified route.

Adding a user directory-based route

Use the following steps to add a user directory-based delivery route on the **Settings** > **Inbound/Outbound** > **Mail Routing** page:

1. Click **Add** to open the Add User Directory-based Route page.
2. Enter a name for your new route in the **Name** field (length between 4 - 50 characters).
3. Select an order number from the **Route order** drop-down list to determine the route's scanning order.

4. Select a destination domain from the pre-defined domains in the **Domain group** drop-down list. Default is Protected Domain. Information about the domain group appears in the Domain details box.

   If you want to edit your selected domain group, click Edit to open the Edit Domain Group page. See *Editing a domain group*, page 52, for details.

5. Select the user directories you want to use to define your route in the User Directories section. Select from the list of currently defined user directories and click the arrow button to move them to the Selected User Directories box.

   Note

   ESMTP user directories are not included in the directory list. ESMTP user directories cannot be used for user directory-based routes.

   If you want to add a new user directory, click **Add user directory** to open the Add User Directory page. See *Adding and configuring a user directory*, page 46, for information.

   If you want to remove a user directory from the Recipients list, select it and click **Delete**.

6. Select the delivery method:

   - Based on the recipient's domain
   - Based on SMTP server IP address designation

     If you select this option, an Add SMTP Server box opens below the option. Enter the SMTP server IP address or host name and port. Mark the check box to enable MX lookup. Click the arrow to add the SMTP server information to the SMTP Server List.

7. Select any desired security delivery options.

   a. Select **Use Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.

   b. Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

Domain-based routes

Delivery routes based on domain groups are scanned after defined user directory-based routes for a match with an email message recipient. If a match is made with a user directory-based route, domain-based routes are not scanned for matches.

Important

The Protected Domain group defined in the **Settings** > **Users** > **Domain Groups** page should not be used to configure Email Security Gateway delivery routes if you need to define domain-based delivery routes via multiple SMTP servers.

Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

Adding a domain-based route

Use the following steps to add a domain-based delivery route on the **Settings** > **Inbound/Outbound** > **Mail Routing** page:

1. Click **Add** to open the Add Domain-based Route page.
2. Enter a name for your new route in the **Name** field.
3. Select an order number from the **Route order** drop-down list to determine the route's scanning order.
4. Select a destination domain from the pre-defined domains in the **Domain group** drop-down list. Default is Protected Domain. Information about the domain group appears in the Domain details box.

   If you want to edit your selected domain group, click Edit to open the Edit Domain Group page. See *Editing a domain group*, page 52, for details.
5. Select the delivery method:
   - Based on the recipient's domain (using the Domain Name System [DNS])
   - Based on SMTP server IP address designation (using smart host). If you select this option, an Add SMTP Server box opens.
     a. Enter the SMTP server IP address or host name and port.
     b. Mark the check box to enable MX lookup.
     c. Click the arrow to add the SMTP server information to the SMTP Server List.

     You may enter no more than 16 addresses in the SMTP Server List.
6. Select any desired security delivery options.
   a. Select **Use Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.

b. Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

Rewriting email and domain addresses

An email envelope recipient address can be rewritten to redirect message delivery to a different address. Envelope sender and message header addresses can also be rewritten to mask address details from message recipients. You can configure address rewriting for inbound, outbound, and internal email on the **Settings > Inbound/Outbound > Address Rewriting** page.

You can export all the email or domain addresses in an address rewrite list to a text file by clicking **Export** when that list is displayed.

Remove an email or domain address from one of your address rewrite lists by selecting it and clicking **Delete**.

Adding recipient address rewrite entries

Use the Inbound Messages tab to specify recipient address rewrite entries for inbound messages and the Outbound and Internal Messages tab for outbound or internal message redirection. The email envelope recipient address is rewritten based on the entries in the Envelope Recipient Address Rewrite List.

Use the following steps to add recipient rewrite entries:

1. Click **Add** in the Envelope Recipient Address Rewrite List to open the Add Recipient Email or Domain Address page.
2. Enter your addresses in 1 of 2 ways:
   - Mark the **Individual email address or domain rewrite entry** check box and enter the original recipient address and the rewrite address in the appropriate entry fields.

     An email address entry may have multiple rewrite entries, with each entry separated by a space. A domain address may have only 1 rewrite entry.
   - If you have an existing email or domain address rewrite entry file, mark the **Email address or domain rewrite entry file** check box and browse to the file.
3. Click **OK**. Your entries appear in the Envelope Recipient Address Rewrite List.

Adding message header address rewrite entries

Use the Inbound Messages tab to add message header address rewrite entries for inbound messages and the Outbound and Internal Messages tab for outbound or internal message address masking. Email Security can rewrite the email envelope

sender address, along with message header addresses, based on the entries in the Envelope Sender and Message Header Rewrite List.

Use the following steps to add address rewrite entries:

1. Click **Add** in the Envelope Sender and Message Header Rewrite List to open the Add Sender Email or Domain Address page.
2. Enter your addresses in 1 of 2 ways:
   - Mark the **Individual email address or domain rewrite entry** check box and enter the original sender address and the rewrite address in the appropriate entry fields.

     Each email or domain address entry may have only 1 rewrite entry.
   - If you have an existing email or domain address rewrite entry file, mark the **Email address or domain rewrite entry file** check box and browse to the file.
3. Click **OK**. Your entries appear in the Envelope Sender and Message Header Rewrite List.

Managing message queues

You can view, create, and configure message queues on the **Main > Message Management > Message Queues** page. You can also modify the following default queues:

- virus
- spam
- exception
- encryption-fail
- decryption-fail
- archive

All blocked messages across all queues are accessed in the **Main > Message Management > Blocked Messages** page (see *Managing the blocked message queue* for details). Temporarily delayed messages can be viewed in the **Main > Message Management > Delayed Messages** page (see *Managing the delayed message queue* for information).

Message queues list

The Queue List on the Message Queues page contains the following information about each queue:

- Queue name. Click a queue name in the Queue List to view and manage the messages in the queue. See *Viewing a message queue*, page 75, for details.

- Queue status, indicating whether the queue is in use or not. Click the **Referenced** link in this column to see a list of the Email Security functions that use the queue. During a queue move operation, an icon in this column indicates whether the move is in progress or has failed.
- Message volume, indicating the total number of messages in that queue
- Size/Total, indicating the queue's current size as a portion of its maximum configured size
- Storage location, showing the location of queue storage (Local, via Network File System [NFS], or via Samba). Icons in this column indicate storage status, such as low disk space or a lost connection.
- The Properties column contains a link to a page displaying the queue's current settings. Click this **Edit** link to change any queue settings.

You can remove a user-created queue by marking the check box next to the queue name in the Queue List and clicking **Delete**. You cannot delete a default queue.

Related topics:

- *Creating a message queue*, page 74
- *Viewing a message queue*, page 75
- *Managing the blocked message queue*, page 76
- *Managing the delayed message queue*, page 78
- *Viewing a message in a queue*, page 80

Creating a message queue

Use the following steps to create a new message queue on the **Main** > **Message Management** > **Message Queues** page:

1. Click **Add** below the Queue List to open the Add Queue page.
2. Enter a name for the new queue in the **Queue name** field.
3. Select the location for this queue's storage.
   - Use **Local** to store the queue locally.
   - Select **Via Network File System (NFS)** to use the NFS protocol for file storage. Enter the IP address or host name of the storage location, along with its shared path.

     Note
     Email Security Gateway supports the use of NFS version 3 or later.

   - Select **Via Samba** to use Samba to facilitate file storage. Enter the following information for Samba:
     - IP address or host name of the storage location
     - Its shared path
     - Username

- Password

4. Configure the maximum number of days a message is retained in the queue, from 1 to 180 days, in the **Maximum message retention** field. Default is 30 for administrator-created queues.
5. Configure the maximum queue size, from 1 to 51200 MB (default is 1024).
6. For an appliance in a cluster, specify the maximum storage size (in MB) assigned to each cluster machine.

Changing message queue properties

To change a message queue's properties, click **Edit** in the Queue List Properties column for that queue to open the Edit Queue page.

Viewing a message queue

Click a queue name in the Message Queues page Queue List to open that queue. Use the **View from/to** fields to specify the desired date/time range for the entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar. Click the arrow to the right of the **View** date/time range to display the desired queue items.

You can also perform a keyword search of the message queue, or refine the search by specifying that only senders, recipients, subjects, or policies applied are searched. You can also search on the name of the appliance that processed the messages (Processed By category). Enter a keyword and click **Search**.

Configure how many messages you want to view on each page of the queue in the **per page** drop-down list (25 [the default], 50, or 100).

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. You can view message information and message contents by clicking the link in the Subject column to open the View Message page. See *Viewing a message in a queue*, page 80.
- Message size
- Date/time of message receipt

- Policy applied to the message. If a Data Security policy is applied to a message, a **View Incident** link opens data loss prevention incident information in Data Security, where the processing of this message occurs.

  This column does not appear in the archive queue.
- Message type (for example, spam, virus, exception, encryption error, or decryption error)
- The name of the appliance that processed the message is included in the **Processed By** column.

You can select a message in the queue and perform the following actions:

Action	Description
Deliver	Deliver the message to its recipient(s).
Delete	Delete the message from the queue.
Reprocess	Delete the message from the queue and restart the email processing function as if Email Security were receiving it for the first time. For the archive queue, this action is called **Process**.
Not Spam	Report that the message should not be classified as spam and release the message for delivery. This option is available only when spam messages are selected.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The More Actions drop-down list includes the following operations:

Action	Description
Resume Processing	A message that has both spam and virus characteristics may be isolated by 1 type of filter before it has been processed by the other type. If the original quarantine is a false positive, use this action to make sure the message is processed by all relevant filters rather than delivered after only the first scan.
Add to Always Block List	Add the message sender to the Always Block List.
Add to Always Permit List	Add the message sender to the Always Permit List.
Forward	Forward the message to 1 or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Clear All Messages	Delete all the messages in the queue.

Managing the blocked message queue

The **Main > Message Management > Blocked Messages** page lists all blocked messages from most queues across all appliances together in a single table, with a

column entry that indicates the name of the queue in which a message is stored. Messages in the archive and Delayed Messages queues are not included on this page.

Use the **View from/to** fields to specify the desired date/time range for the entries you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar. Click the arrow to the right of the **View** date/time range to display the desired queue items.

You can also perform a keyword search of all blocked messages, or refine the search by specifying that only senders, recipients, subjects, or policies applied are searched. You can also search on an individual queue or on the name of the appliance that processed the messages (Processed By category). Enter a keyword and click **Search**.

Configure how many messages you want to view on each page of the queue in the **per page** drop-down list (25 [the default], 50, or 100).

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. You can view message information and message contents by clicking the link in the Subject column to open the View Message page. See *Viewing a message in a queue*, page 80.
- Message size
- Date/time of message receipt
- Policy applied to the message. If a Data Security policy is applied to a message, a **View Incident** link opens data loss prevention incident information in Data Security, where processing this message occurs.
- Queue name (for example, spam, virus, exception, encryption-fail, or decryption-fail)
- Message type (for example, spam, virus, exception, encryption error, or decryption error)
- The name of the appliance that processed the message is included in the **Processed By** column.

You can select a message in the blocked messages queue and perform the following actions:

Action	Description
Deliver	Deliver the message to its recipient(s).
Delete	Delete the message from the queue.
Reprocess	Delete the message from the queue and restart the email processing function as if Email Security were receiving it for the first time.
Not Spam	Report that the message should not be classified as spam and release the message for delivery. This option is available only when spam messages are selected.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The More Actions drop-down list includes the following operations:

Action	Description
Resume Processing	A message that has both spam and virus characteristics may be isolated by 1 type of filter before it has been processed by the other type. If the original quarantine is a false positive, use this action to make sure the message is processed by all relevant filters rather than delivered after only the first scan.
Add to Always Block List	Add the message sender to the Always Block List.
Add to Always Permit List	Add the message sender to the Always Permit List.
Forward	Forward the message to 1 or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.

Managing the delayed message queue

Email that is temporarily undeliverable as a result of various connection issues is sent to the delayed messages queue. Delayed messages may be automatically resent by the system. See *Configuring message delivery options*, page 82, for information about setting the delayed messages delivery retry interval and configuring a notification message to be sent for undelivered email.

Delayed message delivery may also be scheduled for a future date using a custom content filter action. See *Custom Content*, page 88, for information about custom content filters and *Creating and configuring a filter action*, page 93, for details about scheduling a delayed message delivery.

You may view the messages in this queue and perform any necessary processing activities manually on the **Main > Message Management > Delayed Messages** page. When the Delayed Messages page appears, the most recent messages are shown. Use

the **View from/to** fields to specify the desired date/time range for the messages you want to see. The calendar includes the following options:

- Change the month and year by using the back and next arrows around the month and year at the top of the calendar.
- Set the calendar to the current date by clicking the date in the lower left corner of the calendar.
- Click **Clean** to clear the current date/time calendar selection.
- Click **Today** to set the calendar date to today's date.

Set the time range in hours and minutes in the entry fields to the right of the calendar. Click the arrow to the right of the **View** date/time range to display the desired queue items.

You can also perform a keyword search of the message queue, or refine the search by specifying that only senders, recipients, or subjects are searched. If appliances are configured in a cluster, you can also search on the name of the appliance that processed the messages. Enter a keyword and click **Search**.

You can configure the number of messages per page, between 25 and 100, in the **Per page** drop-down list in the queue list banner (25 [the default], 50, or 100).

Information displayed in the list of messages includes the following items:

- Sender email address
- Recipient email address
- Message subject. You can view message information and message contents by clicking the link in the Subject column to open the View Message page. See *Viewing a message in a queue*, page 80.
- Message size
- Date/time of message receipt
- Date of the next scheduled message delivery attempt
- The reason a message is delayed. Entries in this column may be 1 of the following:
  - Exception delay *n*. A temporary delay due to connection issues; *n* is the number of retry attempts remaining for the message.
  - Scheduled delay. An intentional delay that is scheduled via a custom content filter action (see *Creating and configuring a filter action*, page 93, for information).
- The name of the appliance that processed the message is included in the **Processed By** column.

You can select a message in the queue and perform the following actions:

Action	Description
Release	Attempt the message delivery immediately.

Action	Description
Delete	Delete the message from the queue.
Refresh	Refresh the queue contents list to view up-to-date queue contents.

The More Actions drop-down list includes the following operations:

Action	Description
Forward	Forward the message to 1 or more recipients. The forwarded message is added as an attachment to the forwarding message.
Download	Download the message in .eml format. Downloaded email is saved in a zip file.
Release all messages	Attempt to deliver all the messages in the queue.

Viewing a message in a queue

Click the link for a message in the Subject column of a queue to open the View Message page, which contains details about the message as well as the message contents. The **Back** link at the top of the page returns you to the View Queue page. The **Previous** and **Next** links let you navigate to the previous or next message in the queue messages list.

The following information about a selected message is displayed on the View Message page:

Field Name	Description
Sender	Sender's email address
Recipient	Recipient's email address
From	Name of the sender
To	Name of the recipient
Date	Date the message was received
Processed by	Name of the appliance that processed the message
Header	Click the link to view the message header
Attachment	If the message contains an attachment, a link allows you to open it.
Subject	Message subject

The message actions available to you on any View Queue page are also available on the View Message page, except Clear All Messages or Release All Messages. See *Viewing a message queue*, page 75, for descriptions of these actions. You can also choose to view message contents in either text or HTML format, an option in the More Actions drop-down list.

Handling special situations

Some messages require special handling in Email Security Gateway. A message might be undeliverable for example, because of formatting issues, or it might require encrypting or decrypting. See the following topics for detailed information:

- *Configuring exception settings*, page 81
- *Configuring message delivery options*, page 82
- *Handling encrypted messages*, page 83

Configuring exception settings

The **Settings > Inbound/Outbound > Exceptions** page specifies how messages that cannot be processed for some reason are handled in Email Security Gateway. Configure message exception settings as follows:

1. Specify the action to perform on a message that Email Security Gateway cannot process:
   - Deliver the message when an exception is caused by an antivirus filter.
   - Deliver the message when an exception is caused by an antispam filter (default setting).
   - Deliver the inbound message when an exception is caused by Data Security (default setting).
   - Deliver the outbound or internal message when an exception is caused by Data Security.
   - Deliver messages when an exception is caused by any other Email Security Gateway operation.
   - Save exception messages to a queue (default setting).

     Select the desired folder from the drop-down list (default is **exception**). The list includes all the default queue names and any administrator-created queues. If you want to add a new queue, select **Add Folder** from the drop-down list to open the Add Queue screen.

     Warning

     You must have the save option selected in order to save undelivered messages to a queue. If this option is not selected, messages may be dropped from Email Security Gateway.

2. If you want a notification sent regarding the unprocessed message, mark the **Send notification** check box to enable the Notification Properties section.
3. Specify the notification message sender from the following choices:
   - Original email sender (the default)

- Administrator. If you use this option, you must configure a valid administrator email address in the **Settings** > **General** > **System Settings** page (see *Setting system notification email addresses*, page 41).
- Custom. Specify a single email address in this field.

4. Specify 1 or more notification message recipients from among the following choices:
   - Original email sender
   - Original email recipient
   - Administrator (the default). If you use this option, you must configure a valid administrator email address in the **Settings** > **General** > **System Settings** page (see *Setting system notification email addresses*, page 41).
   - User specified. Enter 1 or more email addresses, separated by semicolons, in this field.
5. Specify the subject line of your notification message in the **Subject** field.
6. Enter the body of your notification message in the **Content** field.
7. If you want the original message to be attached to the notification message, mark the **Attach original message** check box.

Configuring message delivery options

Message delivery options help you control the rate of traffic deliveries in your system and how undeliverable mail is handled. Options for these operations appear on the **Settings** > **Inbound/Outbound** > **Delivery** page.

Setting delivery traffic control options

Use the following steps in the Traffic Control section to establish message traffic control limits in your system:

1. Enter the maximum number of simultaneous message deliveries to an individual routing address in the **Maximum number of deliveries** field. Default is 20.
2. Enter the maximum number of message recipients per message in the **Maximum number of recipients** field. Default is 50.
3. If you want to use an SMTP session cache, mark the **Enable SMTP session cache** check box.

Handling undelivered messages

Use the following steps to determine how to handle messages that are temporarily undeliverable due to error situations:

1. In the Undelivered Message Options section, enter the time (in minutes) for the message retry interval in the **Retry interval** field (default is 15).
2. Enter the time (in minutes) for the maximum period for retrying message delivery in the **Maximum retry period** field (default is 1440).

3. In the **Notification email address** field, enter an email address to which you want to send messages that have not been delivered by the end of the retry period.

   Mark the **Use Administrator email address** check box to send these messages to the administrator. If you want to use an administrator address to receive notification messages, you must configure the address in the **Settings** > **General** > **System Settings** page (see *Setting system notification email addresses*, page 41).

   If no address is specified, undelivered mail is returned to the sender.

Handling encrypted messages

An email content policy configured in the Data Security module may specify that a message should be encrypted for delivery. Email Security Gateway supports 3 types of encryption:

- *Mandatory Transport Layer Security (TLS) encryption*
- *Hybrid service encryption*
- *Third-party encryption application*

Use the **Settings** > **Inbound/Outbound** > **Encryption** page to specify the type of encryption you want Email Security to use.

Mandatory Transport Layer Security (TLS) encryption

TLS is an Internet protocol that provides security for all email transmissions—inbound, outbound, and internal.The client and server negotiate a secure “handshake” connection for the transmission to occur, provided both the client and the server support the same version of TLS.

In Email Security, if you select only TLS for message encryption and the client and server cannot negotiate a secure TLS connection, the message is sent to a delayed message queue for a later delivery attempt.

If you select TLS for message encryption, you can also designate either hybrid service or third-party application encryption as a backup method, in case the TLS connection fails. Specifying a backup option allows you a second opportunity for message encryption in the event of an unsuccessful TLS connection. If both the TLS and backup connections fail, the message is sent to a delayed message queue for a later connection attempt.

Select the **Transport Layer Security (TLS)** option to enable TLS encryption. See *Hybrid service encryption*, page 83, and *Third-party encryption application*, page 84, for information about those encryption methods.

Hybrid service encryption

If you want the hybrid service to perform message encryption on outbound messages, mark the **Other encryption methods** check box and then select the **Hybrid service** option on the Encryption page. Hybrid service encryption is available on the **Settings**

> **Inbound/Outbound** > **Encryption** page only if your subscription includes the hybrid service and the hybrid service is registered and enabled.

You can also specify hybrid service encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 83, for details.

When Data Security identifies an outbound message for encryption, the message is sent to the hybrid service via a TLS connection. If the secure connection is not made, the message is placed in a delayed message queue for a later delivery attempt.

The SMTP server addresses used to route email to hybrid service for encryption are configured in the hybrid service setup process. Use the Delivery Route page under **Settings** > **Hybrid Service** > **Hybrid Configuration** to add outbound SMTP server addresses (see *Define delivery routes*, page 30).

If hybrid service detects spam or a virus in an encrypted outbound message, the mail is returned to the message sender.

Hybrid service attempts to decrypt inbound encrypted mail, and adds an x-header to the message to indicate whether the decryption operation succeeded. Message scanning is performed regardless of whether message decryption is successful.

Hybrid service does not encrypt inbound or internal mail. Data Security policy must be modified to designate only outbound messages for encryption when hybrid service is used.

Third-party encryption application

Email Security Gateway supports the use of third-party software for email encryption. The third-party application used must support the use of x-headers for communication with Email Security.

You can also specify third-party application encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 83, for details.

Email Security can be configured to add an x-header to a message that triggers an encryption policy. Other x-headers indicate encryption success or failure. These x-headers facilitate communication between Email Security and the encryption software. You must ensure that the x-header settings made in the Email Security Gateway Encryption page match the corresponding settings in the third-party software configuration, so that Email Security can communicate with the third-party software.

Email Security Gateway x-header settings are entered on the **Settings** > **Inbound/Outbound** > **Encryption** page. Mark the **Other encryption methods** check box and then select the **Third-party application** option to configure the use of external encryption software by Email Security. Use the following steps to configure third-party application encryption in Email Security Gateway:

1. Add encryption servers (up to 32) to the Encryption Server List:
   a. Enter each server's IP address or host name and port number.

b. If you want to use the MX lookup feature, mark the **Enable MX lookup** check box.

c. Click the arrow to the right of the Add Encryption Server box to add the server to the Encryption Server List.

If you want to delete a server from the list, select it and click **Remove**.

2. In the **Encrypted IP address group** drop-down list, specify an IP address group if decryption is enabled or if encrypted email is configured to route back to Email Security. Default is encryption-gateway.
3. If you want users to present credentials to view encrypted mail, mark the **Require authentication** check box and supply the desired user name and password in the appropriate fields. Authentication must be supported and configured on your encryption server to use this function.
4. In the **Encryption X-Header** field, specify an x-header to be added to a message that should be encrypted. This x-header value must also be set and enabled on your encryption server.
5. In the **Encryption Success X-Header** field, specify an x-header to be added to a message that has been successfully encrypted. This x-header value must also be set and enabled on your encryption server.
6. In the **Encryption Failure X-Header** field, specify an x-header to be added to a message for which encryption has failed. This x-header value must also be set and enabled on your encryption server.
7. Select any desired encryption failure options:
   - Mark the **Isolate messages to queue** check box if you want to enable that option. Select a queue for isolated messages from the drop-down list (default is the encryption failure queue).
   - Mark the **Send notification to original sender** check box if you want to enable that option.

     In the Notification Details section, enter the notification message subject and content in the appropriate fields. Mark the **Attach original message** check box if you want the original message included as an attachment to the notification message.
   - Select **Deliver message** (default) if you want the message that failed the encryption operation delivered.
   - Select **Drop message** if you do not want the message that failed the encryption operation delivered.
8. Mark the **Enable decryption** check box if you want Email Security to decrypt encrypted messages.
9. Select any desired decryption options:
   - In the **Content type** field, enter the message content types to decrypt, separated by semicolons. Maximum length is 49 characters. Default entries include multipart/signed, multipart/encrypted, and application/pkcs7-mime.
   - In the **X-Header** field, specify a message x-header that identifies a message to decrypt. This x-header value must also be set and enabled on your encryption server.

- In the **Decryption X-Header** field, specify an x-header to be added to a message that should be decrypted. This x-header value must also be set and enabled on your encryption server.
- In the **Decryption Success X-Header** field, specify an x-header to be added to a message that has been successfully decrypted. This x-header value must also be set and enabled on your encryption server.
- In the **Decryption Failure X-Header** field, specify an x-header to be added to a message for which decryption has failed. This x-header value must also be set and enabled on your encryption server.
- If you want to forward a message that has failed decryption to a specific queue, mark the **On decryption failure** check box, and select a queue for these messages from the drop-down list (default is the decryption failure queue).

5 Working with Filters and Policies

Email Security Gateway lets you define the policies that are applied to specified sets of email senders and recipients. You can create multiple policies for different sets of users in your organization and apply different rules in each policy.

Policy rules comprise the filters and filter actions that determine how a message that matches a policy's sender/recipient conditions is handled. Filters provide the basis for email scanning for viruses and spam, and filter actions determine the final disposition of a message when it triggers a particular filter. Define new filters, or copy and edit an existing filter to suit your organization's needs. Add and define new actions or customize default actions as needed. After you have created and configured filters and filter actions, they are available for inclusion in your policies.

Data Security acceptable use and data loss prevention policies are defined in the TRITON - Data Security module. These policies are enabled or disabled in Email Security Gateway. See *Enabling Data Security policies*, page 96, for more information about these types of policies.

Topics:

Managing filters

Email Security Gateway has 4 predefined default filter types: virus, URL scanning, spam, and disclaimer. The virus filter analyzes an email message and its attachments for the presence of viruses and other threats. URL scanning examines email content for embedded URLs and classifies them according to a database of known spam URLs. The spam filter scans email content and compares it against a database of known spam characteristics. You can select from a variety of antispam tools, including digital fingerprinting, LexiRules, and heuristics scanning tools. If you want to add text at the beginning or end of a message, use the disclaimer filter.

You can also create a custom content filter to scan a message based on message component conditions you configure. Email Security does not provide a custom content filter.

Filters are created and managed via the **Main > Policy Management > Filters** page. Click **Add** to open the Add Filter page and set the properties of your new filter (see *Creating and configuring a filter*, page 88).

You can also copy a filter whether or not it is in use by a policy. A filter can be deleted, as long as it is not in use by any policy. However, you cannot copy or delete an Email Security default filter.

Copying a filter

Copy an existing filter by marking the check box to the left of the filter name to select it and clicking **Copy**. Enter a new filter name in the Copy Filter dialog box, and click **OK**. Click the new filter name in the Filters list to open the Edit Filter page and modify filter attributes.

Deleting a filter

Delete a filter from the Filters list by marking the check box to the left of the filter name and clicking **Delete**. You can delete a filter only if it is not being used by a policy.

Creating and configuring a filter

To create a new filter, click **Add** on the **Main > Policy Management > Filters** page. Enter a filter name and description, then select the filter type you want to use. The filter type you choose determines the filter settings you can configure. Select from the following types:

- *Custom Content*, page 88
- *URL Scanning*, page 90
- *Websense Antivirus*, page 91
- *Websense Antispam*, page 92
- *Disclaimer*, page 92

Custom Content

Use a custom content filter to allow Email Security to scan messages based on conditions you configure. Add or modify a custom content filter on the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page. Email Security does not provide a default custom content filter.

You can choose to trigger your filter on the match of a single condition or the match of all defined conditions by selecting 1 of the following options in the Filter Properties section:

- **Match all conditions**
- **Match any condition**

Specify the conditions of your custom filter from a selection of criteria, including message attributes and operators, by clicking **Add** in the Filter Conditions box. In the Add Condition dialog box, select from among the following message attributes and operators to configure your custom filter (all message attributes except DKIM verification include a user-configurable **Filtering criteria** entry field):

Message Attribute	Operator Options	Additional Options
Sender IP address	Is, Is not	None
Envelope sender	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Envelope recipient	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Number of envelope recipients	Equals, Does not equal, Is less than, is greater than	None
From field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
To field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Cc field address	Contains, Does not contain, Matches regular expression, Does not match regular expression	None
Message subject	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message header: partial	Contains, Does not contain, Matches regular expression, Does not match regular expression	Message attribute text (user configured), Match case
Message header: complete	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case
Message body text	Contains, Does not contain, Matches regular expression, Does not match regular expression	Match case

Message Attribute	Operator Options	Additional Options
Message size	Equals, Does not equal, Is less than, is greater than	Filtering criteria is in KB
DKIM verification result	DKIM verification is successful, DKIM verification failed	None

You can change the order of your filter conditions by marking the check box next to the filter in the Filter Conditions list and clicking **Move Up** or **Move Down**.

Delete a set of filter conditions from the list by marking the check box next to the filter and clicking **Remove**.

> **Note**
> You can use the Add (or Edit) Rule page to add a rule for a custom content filter. You must have already defined a custom content filter before you attempt to add a custom content rule. See *Adding a rule*, page 99, for information.

URL Scanning

URL scanning analyzes email content for embedded URLs and classifies them according to a Websense database of known spam URLs. When you select the URL scanning filter type in the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page, mark the **URL scanning** check box to display a list of URL categories in the Filter Properties area. Select the URL categories that you want Email Security to detect. When the filter detects a URL in a message from a selected category, it applies any configured filter response. This filter is available only when your system includes Websense Web Security and a download server is configured. See *URL scanning with Web Security*, page 36, for more information about integrating with Web Security to use this filter.

> **Note**
> A filter action option of “Resume message scanning” is available so that message scanning can continue after a URL match is detected. See *Creating and configuring a filter action*, page 93, for information.

Select the URL categories for which you want the filter to scan in the **URL Categories** list by marking the appropriate check boxes. Mark the **All** check box to select all URL categories in the list.

Configure any of the following filter responses:

- **Replace matching URLs with.** Mark this check box to enable the filter to replace a URL in a message from a target category with a text string. Enter the replacement text in the entry field to the right of the check box (maximum length is 128 characters).

- **Bypass URL scanning if message size exceeds.** If you want message size to determine whether URL scanning is bypassed, mark this check box and enter a message size in KB (default is 128).

Today and History dashboard charts summarize the instances of embedded URLs that Email Security detects. See *Customizing the Today page*, page 10, for the names of these charts.

Websense Antivirus

Antivirus scanning checks email and any attachments for the presence of email-borne viruses and threats.

Configure how you want the filter to scan messages for viruses from among the **Filter scanning** options:

- **Treat errors as infected**. If antivirus scanning encounters errors, the email is handled as if it is infected. The default setting is on.
- **Treat encrypted files as infected**. A message that is encrypted in a way that the antivirus engine does not understand is treated as infected. The default setting is on.
- **Treat suspicious document as infected.** If antivirus scanning encounters a PDF document that contains active content, including exploits and malicious scripts, the message is handled as if it is infected. Default setting is off.
- **Treat malicious embedded iFrame as infected.** If antivirus scanning detects an HTML page that contains a hidden malicious iFrame, the message is treated as infected. Default setting is off.
- **Scan message body for viruses**. Message content is scanned for embedded malicious scripts or attachments that cannot be scanned properly. If message format problems cause attachments to be seen as part of the message body, the attachments are scanned and viruses detected. Default setting is off.

Configure 1 of the 4 levels of heuristics analysis you want performed in the **Heuristic level** section, from least restrictive (heuristics analysis disabled) to most restrictive. The **Enable normal level of heuristics** is the default setting.

Configure 1 of the following filter responses:

- **Remove infected attachments.** Deletes the attachment that triggers the antivirus filter.
- **Take no action.** This is the default action. The attachment and virus are stored in a predefined location (see *Creating and configuring a filter action*, page 93, for information. If required, a message may be sent to the administrator stating that a virus has been found.

You may also add a notification to a suspected virus email, to alert a recipient that the message may be infected. Use the **Advanced** settings to configure the notification function:

1. Mark the **Notify recipient** check box to enable the notification function.
2. Enter the desired notification text in the entry field below the check box.

3. Specify whether the notification should appear at the top of the message or at the bottom. Default location is at the top of the message.

Websense Antispam

The antispam scanning function checks email for various characteristics of spam. If hybrid service is enabled and configured as a pre-filter in an Email Security Gateway Anywhere environment, it performs antispam scanning. If hybrid service is not configured or available, Email Security Gateway uses a combination of other tools for effective antispam scanning.

Hybrid service analyzes incoming email and blocks any message that it recognizes as spam. Mail that hybrid service allows into the system for processing includes a header that contains a scanning result score. Email Security uses this score to determine how to handle the message. If that score exceeds a specified spam threshold, Email Security treats the message as spam and handles it according to applicable policy. In this case, Email Security Gateway does not perform its own, separate antispam scanning.

Hybrid service must be configured and running for this option to be displayed. Mark the **Use hybrid service scanning results** check box to enable hybrid service spam scoring.

If this check box is not marked (the default) or hybrid service is not enabled, Email Security Gateway performs a complete antispam scan using any or all of the following tools in the Filter Properties Tools list.

- **Digital Fingerprinting scanning.** When enabled, digital fingerprint scanning checks content for any digital fingerprint of known spam.
- **LexiRules scanning.** When enabled, LexiRules scanning analyzes email content for word patterns commonly found in spam.
- **Heuristics scanning.** When enabled, heuristics scanning checks the message header or content for spam characteristics.

  Set the heuristics scanning sensitivity level, from lowest to highest (default is Medium).

If you want message size to determine whether antispam scanning is bypassed, mark the **Bypass antispam scanning if message size exceeds** check box and enter a message size in KB (default is 128).

Disclaimer

The disclaimer filter automatically adds defined text to the beginning or end of a message. Specify the desired text in the Filter Properties section of the Add Filter or Edit Filter page for the Disclaimer filter.

A primary disclaimer may be written in any language, as long as the email message supports the same character set.

The secondary disclaimer must be written in English, to be used when the email does not support the primary disclaimer character set.

Specify where the disclaimer should appear in the email:

- **Beginning of message**
- **End of message**

Mark the **Enable Report Spam feature** check box to allow message recipients to report a message as spam. The link in the disclaimer text sends the recipient to the Personal Email Manager, where the message can be reported from the quarantined message list to Websense as spam.

Managing filter actions

A filter action determines a message's final disposition. Email Security Gateway scans messages and their attachments then performs an action based on applicable policy settings. Actions are created in the **Main > Policy Management > Actions** page. You can add a defined action to a policy rule when you configure your email policies.

Create a new filter action by clicking **Add** and selecting action properties (see *Creating and configuring a filter action*, page 93).

You can remove a filter action by marking the check box to the left of the filter name to select it and clicking **Delete**. You can delete a filter action only if its current status is **Not referenced**. A filter action that is currently referenced by a filter does not have a check box for selection. Note that you cannot remove an Email Security default filter action.

Creating and configuring a filter action

You can add a filter action and configure its properties on the **Main > Policy Management > Actions** page. Click **Add** to open the Add Action page and enter an action name.

Choose from the following 3 message actions:

- **Resume message scanning.** Continue scanning this message using the next filter in sequence if the current filter is triggered. This action may be used if you want message scanning to continue after a URL match is detected in a message. If this option is the final triggered filter's action, the message is delivered.
- **Deliver the filtered message.** (default) Deliver the message to its intended recipient. If you choose this option, you can also define the following message delivery options:
  - **Modify message subject.** Modify the original message subject by adding text to the beginning of it. Mark the **Modify message subject** check box and enter the text you want to add to the message subject.
  - **Add X-header.** Add a specified X-header to any message that triggers the filter associated with this action. Enter only 1 x-header name and value in the **X-header name** and **X-header value** entry fields. The x-header name entry

must begin with “X-”, and both the name and value entries must contain a maximum of 50 alphanumeric characters using ASCII character codes 0 - 127.

- **Delete X-header.** Specify an x-header for deletion by entering only 1 header (without its header value) in the **Delete X-header** entry field. The entry must begin with “X-” and contain a maximum of 50 alphanumeric characters using ASCII character codes 0 - 127.
- **Copy the filtered message to.** Enter at least 1 email address to which you want a copy of the filtered message sent, for example, the email system administrator. Separate multiple email addresses with a semicolon.
- **Delay message delivery until.** Specify a day and time for a delayed message delivery. You may select this option if you want to delay the delivery of a message for some reason. This action option is recommended for use with a Custom Content filter in a policy rule. See *Custom Content*, page 88, for information about a custom content filter.
- **Use IP address**. Specify a standalone appliance IP address from the drop-down list for message delivery. The IP addresses in the list are configured in the V-Series appliance manager. (See *Websense Appliance Manager Help* for information.) This action option is recommended for use with a Custom Content filter in a policy rule. See *Custom Content*, page 88, for information about a custom content filter.

- **Drop the filtered message.** Delete the message without delivering it to its intended recipient.

In addition to the resume processing, deliver message, and drop message actions, the following options are available:

- **Save the original message to a queue.** Send the message to a specified message queue for further processing. Select the **Add Queue** option to add a new queue for this filter action.
- **Send notification.** Sends a predefined notification about the email to specified recipients. If you select this option, configure the notification using the following options:
  - **Sender.** Identify the notification message sender, from among the following options:
    - Original email sender
    - Administrator (default). If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 41).
    - Custom. If you choose this option, you can designate only 1 sender address.
  - **Recipient.** Identify the notification message recipient, from among the following options:
    - Original email sender
    - Original email recipient

  - Administrator. If you use this option, you must configure a valid administrator email address in the **Settings > General > System Settings** page (see *Setting system notification email addresses*, page 41).
  - Custom. If you choose this option, you can designate 1 or more recipient addresses, separated by semicolons.
- **Subject.** Enter the subject that you want to be displayed when the notification is received. The default subject is "WARNING: Message may contain malicious content."
- **Content.** Enter the text that you want to be displayed in the notification message body.
- **Attachment.** Specify whether you want to include the original message as an attachment to the notification message. Select from among the following:
  - Do not attach message (default)
  - Attach original unfiltered message
  - Attach filtered message

Editing an existing filter action

You can edit an existing filter action by clicking the action name on the **Main > Policy Management > Actions** page. The Edit Action page opens, displaying the current action properties. Modify any of the options listed in *Creating and configuring a filter action*, page 93.

Managing policies

An Email Security Gateway policy is applied based on defined sender/recipient conditions and the direction of the email. You can apply a different policy to different groups of senders and recipients. For example, you might apply a policy to a marketing department group in your organization and a different policy to a human resources group. After you define a set of senders and recipients in a policy, you can add the policy rules (a combination of filter and filter action) to apply when the sender/recipient conditions of the email match the policy.

Email Security has 3 general types of policies, depending on the direction of the email—inbound, outbound, or internal. Message direction is determined on the basis of an organization's protected domains:

- Inbound - The sender address is not from a protected domain, and the recipient address is in a protected domain
- Outbound - The sender address is from a protected domain, and the recipient address is not in a protected domain
- Internal - Both the sender and recipient addresses are in a protected domain.

Email Security Gateway has 1 predefined default policy for each email direction, as well as a default Data Security policy for each direction.

Data Security policies may be applied to email in any direction. These policies are configured in the Data Security module of TRITON Unified Security Center and can only be enabled or disabled in Email Security Gateway. You need to register Email Security with the Data Security management server and click **Deploy** in the Data Security module for the policies to be active. See *Enabling Data Security policies*, page 96 for details.

Changing policy order

After you add a policy, you can select it and use the **Move Up** and **Move Down** buttons to move it up or down in the policy list in order to specify when the policy is applied. When message conditions match a policy, subsequent policies in the list are not applied.

You cannot change the order of default policies. They are applied last when a message matches no other policy.

Deleting a policy

You can remove a policy by marking the check box next to the policy name on the Policies page and clicking **Delete**. Note that a default policy cannot be deleted.

Related topics:

- *Enabling Data Security policies*, page 96
- *Creating a policy*, page 97
- *Adding Sender/Recipient Conditions*, page 98
- *Editing rules*, page 99

Enabling Data Security policies

In addition to creating and enabling policies that protect your email system from viruses and spam, you can enable Websense Data Security policies that can detect the presence of sensitive data in your organization's email and execute appropriate actions to prevent data loss. You can use Data Security policies for inbound, outbound, and internal email.

The Data Security Email Data Loss Prevention policy must be configured in the Websense Data Security module. See *TRITON - Data Security Help* for detailed information.

Data Security policies are enabled by default in Email Security Gateway. However, Email Security must be registered with the Data Security Management Server before the policies are applied to email. See *Registering with Websense Data Security*, page 34, for instructions on how to register with Data Security.

If you need to enable Data Security policies in Email Security Gateway for some reason, click the Data Security policy name on the **Main > Policy Management > Policies** page for inbound, outbound, or internal email, and set the following options in the Edit Policy page:

- **Status:** Enabled or Disabled. Enable or disable the Data Security policy in Email Security. Data Security policies are enabled by default.
- **Mode:** Monitor or Enforce. Select **Monitor** if you want Data Security to simply monitor your email, and select **Enforce** if you want Data Security to apply its policies to your email.
- **Notification.** Add a notification to a message when an email attachment to that message has been dropped as a result of a Data Security policy.
  1. Mark the **Send notification when attachment of the message is dropped** check box to enable the sending of notifications.
  2. Enter the notification message text.
  3. Determine whether the notification text appears above or below the message body of the mail whose attachment was dropped.

> **Note**
> A message that triggers a Data Security policy whose action is Quarantine is isolated in the Data Security quarantine queue, not in an Email Security Gateway queue. The message can be released for delivery by Data Security.

Creating a policy

Use the **Main > Policy Management > Policies** page to create a new inbound, outbound, or internal policy.

1. Click **Add** to open the Add Policy page and enter a unique **Policy name**. The policy name must be between 4 and 50 characters long. Use of the following special characters in the policy name is not recommended:

   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,

   Policy names can include spaces, dashes, and apostrophes.
2. Enter a clear and concise **Description** of the policy.

   The special character recommendations that apply to policy names also apply to descriptions.
3. Define the order in which this policy is applied in the **Order** field.

   By default the new policy is placed at the top of the list. You cannot have multiple policies with the same order number. If you select a number that is already in use, the policy that currently has that number and all those below it move down 1 place in the list.
4. Define your **Sender/Recipient Conditions**.

By default, each new policy contains a sender/recipient condition that applies the policy to all email senders and recipients. To add more conditions click **Add**, and then see *Adding Sender/Recipient Conditions*, page 98.

> **Note**
> You must define a sender/recipient condition. A policy that does not contain a sender/recipient condition will not be applied.

5. Edit the available **Rules** to tailor the filters and actions to this policy. Click a rule name, and then see *Editing rules*, page 99.
6. Click **OK** to save your policy.

Adding Sender/Recipient Conditions

Use the **Add Policy** > **Add Sender/Recipient Condition** page to specify the sender(s) and recipient(s) to which this policy applies. You can make the policy as wide-ranging as required, for example applying it to all users, or all users receiving mail in a particular domain, or specific email addresses only.

For each sender/recipient condition, you must select a **Sender Source** and **Recipient Source**:

- If you select **Local Address**, enter the sender or recipient email addresses to use with the policy. You can use the asterisk wildcard to specify combinations, for example:
  - *.mycompany.com applies the policy to all users with a mycompany.com email address
  - *sales@mycompany.com applies the policy to a subset of all email addresses in mycompany.com, such as us_sales@mycompany.com and uk_sales@mycompany.com
  - john.doe@mycompany.com applies the policy to a specific user.

  To apply the policy to all email addresses, enter an asterisk (*).
- If you select **User directory**, select the directory source from the drop-down list. You must set up a user directory to connect to before selecting this option. Select **Add User Directory** to create a new directory source.

Once you have made your selections, click **OK** to return to the Add or Edit Policy page.

Deleting Sender/Recipient Conditions

To delete a sender/recipient condition, on the Add or Edit Policy page check the box next to the condition ID and then click **Delete**.

A policy that does not contain any sender/recipient conditions will not be applied to an email message.

Adding a rule

A policy rule comprises the filter applied to a message that matches a policy's sender/recipient conditions and the Email Security action taken when that message triggers the filter. You may create a new rule only in combination with a custom content filter.

Use the following steps to add a policy rule with a custom content filter:

1. Click **Add** in the Rules section to open the Add Rule page.
2. Enter a name for your rule in the **Rule Name** entry field.
3. Select the desired policy status, **Enabled** (the default) or **Disabled**.
4. Select the order in which you want your rule applied. By default, a new custom content rule is created in the first position. Use the **Move Up** and **Move Down** buttons to adjust custom content rule order. The Disclaimer rule is always applied last.
5. Select a custom content filter from the **Filter name** drop-down list. If you have not created a custom content filter, this list contains only the entry **Add filter**. Choose this entry to open the Add Filter page to define a new custom content filter. The filter type is always **Custom Content**. See *Creating and configuring a filter*, page 88, for information.
6. Configure a filter action in 1 of the following ways:
   - Select a default filter action from the **Action name** drop-down list. If you want to change the default action settings, click **Edit**.
   - You can also create a new action for your rule by selecting **Add Action** from the drop-down list.

   See *Creating and configuring a filter action*, page 93, for information.

Editing rules

Click a rule name, and use the **Add Policy > Edit Rule** page to define what happens to an email message that matches the sender/recipient conditions and triggers the policy. This page contains the filter and filter action that currently define the rule that you clicked. You can also define message sender/recipient conditions that, when met, allow a message to bypass the filter.

Editing the filter

To edit the filter, click **Edit** in the Filter section to open the Edit Filter page. Modify filter characteristics as described in *Creating and configuring a filter*, page 88.

Editing the filter action

To edit the filter action, click **Edit** in the Action section to open the Edit Action page. Modify action options as described in *Creating and configuring a filter action*, page 93.

> **Note**
> Any change you make to existing rule components will be reflected in the filter and action definitions you configured in the **Main > Filters** and **Main > Actions** pages. The changes are not unique to the individual policy.

Adding filter bypass conditions

To add filter bypass conditions, click **Add** in the Filter Bypass Condition section to open the Add Filter Bypass Conditions page. You can create filter bypass entries in both the Sender Email Addresses and Recipient Email Addresses sections in 1 of the following ways:

- Add a predefined email address list by clicking **Browse** next to the Email Address File field and navigating to the desired text file. The file format should be 1 email address per line, up to a maximum of 8 addresses.
- Enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.

An asterisk (*) may be used in an address as a wildcard.

Click **OK** to save your bypass entries.

You can delete an entry in an Email Address List by selecting it and clicking **Remove**. Export and save an address list as a text file by clicking **Export All**.

You cannot use these settings to bypass a custom content filter.

Editing an existing policy

You can edit an existing policy by clicking its name on the Policies page to open the Edit Policy page. Edit the Description, Status, Sender/Recipient Conditions, and Rules as described in *Creating a policy*, page 97. You will not be able to edit the policy name.

You can edit policy order only for a policy you have created. You cannot edit policy order for a default policy.

Managing global Always Block and Always Permit lists

Maintaining lists of IP and email addresses that are either always blocked or always permitted can contribute to the efficiency of your Email Security Gateway system.

Bandwidth and time can be saved when trusted mail can bypass the system's spam and virus scanning features.

> **Note**
> Mail from addresses in the global Always Permit lists is subject to other Email Security Gateway filtering, including message control, connection control, directory harvest attack, and relay control.

Managing the Always Block List

You can add an IP or email address directly into the Always Block List from the **Main > Policy Management > Always Block/Permit** page. You can also add a predefined IP or email address list, remove individual entries from a list, export a list to your desktop as a text file, and search a list.

Messages from an email address that appears in both the Always Block and Always Permit lists will be permitted. Messages from an IP address that appears in both lists will be blocked.

After you finish adding your address entries, you can export the list as a text file by clicking the **Export All** button and opening your text file or saving it to a desired location.

Remove an individual entry by selecting it in the IP or Email Address List and clicking **Remove**. You can also search your list for entries by entering keywords in the search field and clicking **Search**.

Adding an IP address to the Always Block List

Use the following procedures to add IP addresses to the Always Block list:

1. Click the **Always Block** tab.
2. In the IP Address Block List section of the page, add a predefined IP address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 IP address per line.
3. You can also enter an individual IP/subnet address in the **IP/Subnet address** field. Click the right arrow button to add the individual entry to the **IP Address List** on the right.
4. Click **OK**.

Adding an email address to the Always Block List

Use the following procedures to add email addresses to the Always Block list:

1. Click the **Always Block** tab.
2. In the Email Address Block List section, add a predefined email address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 email address per line.

3. You can also enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.
4. Click **OK**.

Managing the Always Permit List

You can add an IP or email address directly into the Always Permit List from the **Main > Policy Management > Always Block/Permit** page. You can also add a predefined IP or email address list, remove individual entries from a list, export a list to your desktop as a text file, and search a list.

Email from an address that appears in both the Always Block and Always Permit lists will be permitted. Messages from an IP address that appears in both lists will be blocked.

After you finish adding your address entries, you can export the list as a text file by clicking the **Export All** button and opening your text file or saving it to a desired location.

Remove an individual entry by selecting it in the IP or Email Address List and clicking **Remove**. You can also search your list for entries by entering keywords in the search field and clicking **Search**.

Adding an IP address to the Always Permit List

Use the following procedures to add IP addresses to the Always Permit List:

1. Click the **Always Permit** tab.
2. In the IP Address Permit List section of the page, add a predefined IP address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 IP address per line.
3. You can also enter an individual IP/subnet address in the **IP/Subnet address** field. Click the right arrow button to add the individual entry to the **IP Address List** on the right.
4. Click **OK**.

Adding an email address to the Always Permit List

Use the following procedures to add email addresses to the Always Permit list:

1. Click the **Always Permit** tab.
2. In the Email Address Permit List section, add a predefined email address list by clicking **Browse** and navigating to the desired text file. The file format should be 1 email address per line.
3. You can also enter an individual email address in the **Email address** field. Click the right arrow button to add the individual entry to the **Email Address List** on the right.
4. Click **OK**.

Enabling the Dynamic Always Permit List

Enabling the Dynamic Always Permit List function allows some mail exchanged between a sender/recipient address pair to bypass antispam filtering. When mail between a sender to a recipient does not trigger an antispam filter a specified number of times, that sender/recipient address pair is added to the Dynamic Always Permit List. Antispam filtering is not performed on mail between this sender/recipient address pair. When a specified timeout period has elapsed, the address pair is removed from the list.

The **Enable Dynamic Always Permit list** check box is enabled by default in the Dynamic Always Permit List section. The following settings can be modified:

1. In the **Occurrence** field, specify the number of spam-free email exchanges (from 1 to 5) required before a sender/recipient pair is added to the list. Default is 1.
2. In the **Timeout** field, enter a value for the timeout interval in hours (from 1 to 720). Default is 720.

Clear the list manually by clicking the **Clear Dynamic Always Permit List** button. Note that if you disable this function, the list is automatically cleared.

6 Working with Reports

Email Security Gateway logs and collects data about email traffic and system activity to generate presentation reports and Today/History page dashboard charts and statistics. Data is sent to the Log Database for storage, where it is accessed to generate a variety of reports and charts. This chapter covers Log Database configuration and maintenance options and how to change the location of the database. Report settings that determine how a report is distributed and how long it is stored in the system are explained. Customizing a report template and scheduling and running a presentation report are also described.

Topics:

Configuring Log Database options

The Log Database stores the records of email traffic activity and the associated Email Security Gateway filtering actions on that traffic. These data records are used to generate presentation reports of Email Security activity, including size and volume of email messages and identification of senders and recipients. They are also used to generate the status charts on the Today and History dashboards.

Administering the Log Database involves controlling many aspects of database operations, including the timing of maintenance tasks, the conditions for creating new database partitions, and which partitions are available for reporting. Use the **Settings** > **Reporting** > **Log Database** page to manage Log Database operations.

Click the **OK** button within each section of the Log Database page to save and implement the changes in that section.

A Log Database Location section at the top of the page lets you enter the IP address\instance or host name\instance of your Log Database server. By default, the Log Database created at installation is entered. If you chose to encrypt the database connection at product installation, the **Encrypt connection** check box is marked. If

you did not select the encryption option during installation, you can encrypt the database connection by marking the check box here.

> **Important**
> You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.

Other settings created at installation and displayed here include the designated authentication method (Windows or SQL Server), user name, and password.

Click **Check Status** to determine the availability of the server.

The top of the Log Database Options section displays the name of the active Log Database and a Refresh link. Click **Refresh** to update the information shown on the Log Database page. Be sure you save your settings before you click **Refresh**, because any unsaved changes on the page will be cleared.

Use the Database Rollover Options section of the **Settings > Reporting > Log Database** page to specify when you want the Log Database to create a new database partition, a process called a roll over.

Use the **Roll over every** option to indicate whether database partitions should roll over based on size (MB) or date (weeks or months).

- For size-based rollovers, select MB and specify the number of megabytes the database must reach for the rollover to begin, from 100 - 10240 MB (default is 5120).
- For date-based rollovers, select either weeks or months as the unit of measure, and specify how many full calendar weeks (from 1 - 52) or months (from 1 - 12) to keep in a database partition before a new one is created.

> **Note**
> If the rollover begins during a busy part of the day, performance may slow during the rollover process.
>
> To avoid this possibility, some environments choose to set the automatic rollover to a long time period or large maximum size. Then, they perform regular manual rollovers to prevent the automatic rollover from occurring.
>
> See *Creating database partitions*, page 108, for information on manual rollovers.
>
> Keep in mind that extremely large individual partitions are not recommended. Reporting performance can slow if data is not divided into multiple, smaller partitions.

When a new database partition is created, reporting is automatically enabled for the partition (see *Enabling database partitions*, page 109).

Click **OK** to activate changes to the database rollover options.

Configuring maintenance options

Use the Maintenance Configuration section of the **Settings > Reporting > Log Database** page to control certain aspects of database processing, such as the time for running the database maintenance job, some of the maintenance tasks performed, and deletion of database partitions and error logs.

1. For **Maintenance start time**, select the time of day for running the database maintenance job. Default value is 1:00.

   The time and system resources required by this job vary depending on the tasks you select in this area. To minimize any impact on other activities and systems, it is best to run this job during a slow email traffic period.

2. Mark the **Automatically delete a partition with an end date older than** check box, and then specify the number of days (from 1 to 365) after which partitions should be deleted (default is 365).

   

   Warning

   After a partition has been deleted, the data cannot be recovered. See *Enabling database partitions*, page 109, for an alternative way to delete partitions.

3. Mark the **Enable automatic reindexing of partitions on** check box, and then select a day of the week to have this processing performed automatically (default is Saturday).

   Reindexing the database is important to maintain database integrity and to optimize reporting speed.

   

   Important

   It is best to perform this processing during a quiet time for email traffic. Reindexing database partitions is resource intensive and time consuming. Reports should not be run during the reindexing process.

4. Mark the **Delete failed batches after** check box and then enter a number of days (from 1 to 365) after which to delete any failed batches. Default value is 20.

   If this option is not checked, failed batches are retained indefinitely for future processing.

   If there is insufficient disk space or inadequate database permissions to insert log records into the database, the records are marked as a failed batch. Typically, these batches are successfully reprocessed and inserted into the database during the nightly database maintenance job.

   However, this reprocessing cannot be successful if the disk space or permission problem is not resolved. Additionally, if the **Process any unprocessed batches** option is not selected, failed batches are never reprocessed. They are deleted after the time specified here.

5. Mark the **Process any unprocessed batches** check box to have the nightly database maintenance job reprocess any failed batches.

   If this option is not checked, failed batches are never reprocessed. They are deleted after the time specified in step 4, if any.

6. Mark the **Delete the log after** check box, and then enter a number of days (1 to 120) after which to delete database error records. Default value is 45.

   If this option is not checked, error logs are retained indefinitely.

7. Click **OK** to activate changes to the maintenance configuration options.

Creating database partitions

Database partitions store the individual log records of email traffic activity. Microsoft SQL Server users can configure the Log Database to start a new partition based on partition size or a date interval (see *Configuring Log Database options*, page 105, for more information).

When partitions are based on size, all incoming log records are inserted into the most recent active partition that satisfies the size rule. When the partition reaches the designated maximum size, a new partition is created for inserting new log records.

When the partitions are based on date, new partitions are created according to the established cycle. For example, if the rollover option is monthly, a new partition is created as soon as any records are received for the new month. Incoming log records are inserted into the appropriate partition based on date.

Database partitions provide flexibility and performance advantages. For example, you can generate reports from a single partition to limit the scope of data that must be analyzed to locate the requested information.

Use the Database Partition Creation section of the **Settings > Reporting > Log Database** page to define characteristics for new database partitions, such as location and size options. This area also lets you create a new partition right away, rather than waiting for a planned rollover (see *Configuring Log Database options*, page 105).

1. Enter the file path for creating both the data and log files for new database partitions.
2. Under **Initial Size (MB)**, set the initial file size (from 100 to 2048 MB) for both the Data and Log files for new database partitions.

   

   Note

   Best practice recommends calculating the average partition size over a period of time. Then, update the initial size to that value. This approach minimizes the number of times the partition must be expanded, and frees resources to process data into the partitions.

3. Under **Growth (MB)**, set the increment by which to increase the size (from 8 - 512 MB) of a partition's data and log files when additional space is required.
4. Click **OK** to implement the path, size, and growth changes entered.

Database partitions created after these changes use the new settings.

5. Click **Create** to create a new partition immediately, regardless of the automatic rollover settings.

   To have the new partition use the changes made in this section, be sure to click **OK** before you click **Create**.

   Click the **Refresh** link in the content pane periodically. The Available Partitions area will show the new partition when the creation process is complete.

If you later change the partition file path, you should be sure that the new database folder exists with write privileges.

Enabling database partitions

The Available Partitions section of the **Settings > Reporting > Log Database** page lists all the database partitions available for reporting. The list shows the dates covered by the partition, as well as the size and name of each partition.

Use this list to control what database partitions are included in reports, and to select individual partitions to be deleted.

1. Mark the check box in the **Enable** column next to each partition you want included in reports.

   Use the **Select all** and **Select none** options above the list, as appropriate.

   You must enable at least 1 partition for reporting. Use the **Select none** option to disable all partitions at 1 time so that you can enable just a few.

   Use these options to manage how much data must be analyzed when generating reports and speed report processing. For example, if you plan to generate a series of reports for June, select only partitions with dates in June.

   

   Important

   This selection affects scheduled reports as well as reports that are run interactively. To avoid generating reports with no data, make sure the relevant partitions are enabled when reports are scheduled to run.

2. Click the **Delete** option beside a partition name if that partition is no longer needed. The partition is actually deleted the next time the nightly database maintenance job runs.

   

   Warning

   Use this option with care. You cannot recover data from deleted partitions.

   Deleting obsolete partitions minimizes the number of partitions in the Log Database, which improves database and reporting performance. Use this Delete option to delete individual partitions as needed. See *Configuring maintenance options*, page 107, if you prefer to delete older partitions according to a schedule.

3. Click **OK** to activate changes to the available partitions options.

Viewing log activity

Use the Log Activity section of the **Settings > Reporting > Log Database** page to review database maintenance status and event and error messages recorded during the jobs run on the Log Database. Use the **View** drop-down list to select the maximum number of messages to display.

Changing the Log Database

The Log Database may need to be changed when 1 of the following situations occurs:

- The database IP address changes.
- The database username and password change.
- The user wants to change authentication settings.
- The user wants to use a named instance.

This type of change must be made in 2 locations: in the **Settings > Reporting > Log Database** page and in the Email Security Log Server Configuration wizard.

Use the following steps to change the Log Database configuration:

1. Enter the IP address for the new Log Database in the **Settings > Reporting > Log Database** page, in the **Log database** field.
2. Open the Email Security Log Server Configuration wizard for the Windows machine on which Log Server is installed (**Start > All Programs > Websense > Email Security > Email Security Log Server Configuration**).
3. In the Database tab, click **Connection** to open the Select Data Source dialog box.
4. Select the Machine Data Source tab and click **New** to open the Create New Data Source dialog box.
5. Select **System Data Source (Applies to this machine only)**, and click **Next**.
6. Select **SQL Server** and click **Next**.
7. Click **Finish**.
8. In the Create a New Data Source to SQL Server dialog box, enter the server name, description, and IP address of the new SQL Server database in the **Name**, **Description**, and **Server** entry fields and click **Next**.
9. Select **With SQL Server authentication using a login ID and password entered by the user**.
10. Enter the username (**sa**) and a password and click **Next**.
11. In the **Change the default database to** drop-down list, select the **esglogdb76** database and click **Next**.
12. Click **Finish**.
13. In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** to test the server connection.

14. Click **OK**.
15. Enter the new username and password in the SQL Server Login dialog box.
16. In the Email Security Log Server Configuration wizard Database tab, notice that the ODBC Data Source Name (DSN) field contains the new server name, and click **Apply** to confirm the new configuration.
17. Click **OK** in the warning message. The Log Server must be stopped and restarted for the new settings to take effect.
18. In the Email Security Log Server Configuration wizard Connection tab, click **Stop** to stop the Log Server service.
19. In the same tab, click **Start** to restart the Log Server service. The new database settings are in effect.

Viewing Log Server settings

Use the **Settings** > **Reporting** > **Log Server** page to view the Log Server IP address or host name and port number. Click **Check Status** to determine the availability of the server.

Configuring reporting preferences

Reporting preference settings determine how a scheduled report is distributed for review. You can also specify how long to retain a scheduled report and how much warning administrators receive before a report is deleted.

Use the **Settings** > **Reporting** > **Preferences** page to provide information used to distribute completed scheduled reports via email. Also define how long scheduled presentation reports are stored before they are deleted automatically, and how far in advance to warn administrators that reports are due to be deleted.

1. Enter the email address to appear in the From field when scheduled reports are distributed via email.
2. Enter the SMTP server IP address or name for the email server used to distribute scheduled reports via email.
3. Use the **Store reports for** drop-down list to indicate how long scheduled reports are stored on the TRITON – Email Security machine (default is 5 days).

   Note that as you increase the length of time that reports are stored, you affect the amount of disk space required on the TRITON – Email Security machine. This machine is not an appropriate location for a long-term reporting archive.

   Note

   If you reduce the report storage time after you have started to generate reports, stored reports that exceed this interval will be automatically deleted.

4. Use the **Give administrators this much warning before a scheduled report is deleted** drop-down list to indicate how much warning (from 1 - 5 days) an administrator should have before a report is deleted (default is 3 days).

   The warning is intended to give administrators time to archive important reports in an appropriate location before they are deleted from the TRITON – Email Security machine.

5. Click **OK** to implement your changes.

Working with presentation reports

Presentation reports include a set of predefined charts and tabular report templates with which you can generate graphical reports of Email Security Gateway message traffic activities. You can run a report, customize a report template, or mark a frequently used report as a Favorite. You can run any presentation report immediately, or schedule it to run at a particular time or on a repeating cycle.

Not all report templates can be customized. Report templates that can be customized display a different icon from reports that cannot be customized. If the **Save As** button is enabled when you select a report name, then you can save and edit that report to suit your needs. The **Save As** button is not enabled if you select a report that cannot be customized.

Use the **Main > Status > Presentation Reports** page to generate charts and tabular reports based on templates in the Report Catalog.

The Report Catalog organizes a list of predefined report templates and custom reports into groups. Expand a group to see its corresponding templates and custom reports. Click on a template or report title to see a brief description of what it includes.

To run a presentation report, select the desired report template in the Report Catalog, click **Run**, and then follow the instructions given in *Running a presentation report*, page 118.

To use an existing report as a starting point for creating a report variation, select a custom report, and then click **Save As,** if this button is enabled. If the Save As button is not enabled when you select the report, you cannot edit the template. See *Copying a custom presentation report*, page 113, for detailed instructions.

To make changes to the report filter applied to any custom report you have created, select the report title in the Report Catalog, and then click **Edit**. You cannot modify or delete predefined report templates.

Reports that are used frequently can be marked as Favorites to help you find them more quickly. Just click the report title in the Report Catalog, and then click **Favorite** (see *Working with Favorites*, page 117). Mark **Show Only Favorites** to display only templates that you have marked as Favorites in the Report Catalog.

To delete a custom report you have created, click **Delete**. If a deleted report appears in any scheduled jobs, it will continue to be generated with that job. See *Viewing the scheduled jobs list*, page 124, for information on editing and deleting scheduled jobs.

Use the buttons at the top of the page to schedule reports to run later, view scheduled report jobs, and view and manage reports created by the scheduler.

- Click **Job Queue** to see and manage a list of existing scheduled jobs, along with the status of each job. See *Viewing the scheduled jobs list*, page 124.
- Click **Scheduler** to define a job containing 1 or more reports to be run at a specific time or on a repeating schedule. See *Scheduling a presentation report*, page 119.
- Click **Review Reports** to see and manage a list of reports that were successfully scheduled and run. See *Reviewing scheduled presentation reports*, page 125.

Related topics:

- *Copying a custom presentation report*, page 113
- *Defining the report filter*, page 114
- *Working with Favorites*, page 117
- *Running a presentation report*, page 118
- *Scheduling a presentation report*, page 119
- *Viewing the scheduled jobs list*, page 124
- *Reviewing scheduled presentation reports*, page 125

Copying a custom presentation report

Use the **Save As New Report** page to create an editable copy of a custom report template. Not all templates can be used to create a new custom report. Use the following steps to copy a custom presentation report:

1. Select the custom report in the Report Catalog and, if it is enabled, click **Save As**. If the **Save As** button is not enabled, you cannot copy and customize the selected report.
2. In the **Presentation Reports > Save As New Report** page, replace the report catalog name with a name that will make it easy to identify the new report. (The default name is the name of the original report template, with a number appended to indicate that it is a copy.) The name must be unique and can have up to 85 characters.
3. Click either **Save** or **Save and Edit**.
   - If you click **Save**, you are returned to the Presentation Reports page, where the new report appears in the Report Catalog. To customize the report at any time, select its name, and then click **Edit**.
   - If you click **Save and Edit**, you are taken directly to the Edit Report Filter page. The new report is also added to the Report Catalog.
4. Edit the report filter to modify the report. The report filter controls elements such as which email senders or recipients are included in your custom report.

   For instructions, see *Defining the report filter*, page 114.

Defining the report filter

Report filters let you control what information is included in a report. For example, you might choose to limit a report to selected email senders, email recipients, or message scanning results (such as clean, virus, spam, or Data Security). You can also give a new name and description for the entry in the Report Catalog, change the report title, specify a custom logo to appear, and designate the new report as a Favorite.

> **Note**
> Using a custom logo requires some preparation before you define the report filter. You must create the desired graphic in a supported graphic format and place the file in the appropriate location. See *Customizing the report logo*, page 115.

The filter for predefined report templates cannot be changed. You can edit the filter for a custom report when you create it by choosing **Save and Edit** on the Save As New Report page, or select the report in the Report Catalog at any time and click **Edit**.

The Edit Report Filter page has separate tabs for managing different elements of the report. Select the items you want on each tab, then click **Next** to move to the next tab. For detailed instructions on completing each tab, see:

- *Setting general report options*, page 114
- *Selecting email senders for the report*, page 115
- *Selecting email recipients for the report*, page 116
- *Selecting message scanning results for the report*, page 116

On the Save tab, choose whether to run or schedule the report, and save the report filter. See *Saving the report filter definition*, page 117.

Setting general report options

Use the General tab of the **Presentation Reports** > **Edit Report** page to configure general report characteristics, as follows:

1. Modify the name that appears in the Report Catalog for this report by entering a new name in the **Report catalog name** entry field. The name can have up to 85 characters.

   This name does not appear on the report itself; it is used only for identifying the unique combination of report format and filter in the Report Catalog.
2. Modify the title that actually appears on the report in the **Report title** entry field. The title can have up to 85 characters.
3. Use the **Description** field to modify the brief report description that appears in the Report Catalog. The description can have up to 336 characters.

   The description should help you identify this unique combination of report format and filter in the Report Catalog.

4. Use the **Logo** drop-down list to specify a logo for your report. The default entry is **Websense Logo**. Select **No Logo** if you do not want a logo displayed on this report.

   The list also contains filenames for custom logo image files if you have created and stored supported image files in the appropriate directory. See *Customizing the report logo*, page 115.

5. Mark the **Save as Favorite** check box to have the report selected as a Favorite.

   The Report Catalog shows a star symbol beside Favorite reports. You can select Show only Favorites on the Report Catalog page to reduce the number of reports listed, which enables you to move more quickly to a particular report.

6. After all entries and selections are complete, click **Next** to open the Senders tab.

Customizing the report logo

By default, presentation reports display the Websense logo in the upper left corner. When you create a custom report and edit its report filter, you can choose a different logo, which you have already prepared and copied to the appropriate directory, as follows:

1. Create an image file in one of the following formats:

   .bmp, .gif, .jfif, .jpe, .jpeg, .jpg, .png, .ttf

   Use a maximum of 25 characters for the image file name, including the file extension.

2. Copy the image file to the following default installation directory (or to your own installation directory):

   C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\PRTemplate\jasperreports\images

   All supported image files in this directory automatically appear in the **Logo** drop-down list on the General tab of the Edit Report Filter page. The image is automatically scaled to fit within the space allocated for the logo. (See *Setting general report options*, page 114.)

Selecting email senders for the report

The Senders tab of the **Presentation Reports > Edit Report** page lets you control which senders are included in the report data. You can select only 1 type of sender for each report.

No selections are required on this tab if you want to report on all senders.

1. Select a sender type from the drop-down list.
2. Set the maximum number of search results from the **Search limits** drop-down list (from 10 - 5000). Default value is 10.

   Depending on the email traffic in your organization, there may be large numbers of users, groups, or domains in the Log Database. This option manages the length of the results list, and the time required to display the search results.

3. Enter 1 or more characters for searching, and then click **Search**.

Use an asterisk (*) as a wildcard to signify missing characters. For example, J*n might return Jackson, Jan, Jason, Jon, Joan, and so forth.

Define your search string carefully, to ensure that all desired results are included within the number selected for limiting the search.

4. Highlight 1 or more entries in the results list, and click the right arrow button (>) to move them to the Selected Senders List.
5. Repeat steps 2 - 4 as needed to conduct additional searches and add more senders to the Selected Senders List.
6. To delete an entry from the Selected Senders List, select the entry and click **Remove**.
7. After you are finished making selections or deletions, click **Next** to open the Recipients tab.

Selecting email recipients for the report

The Recipients tab of the **Presentation Reports > Edit Report** page lets you control which recipients are included in the report data. You can select only 1 type of recipient for each report.

No selections are required on this tab if you want to report on all recipients.

1. Select a recipient type from the drop-down list.
2. Set the maximum number of search results from the **Search limits** drop-down list (from 10 - 5000). Default value is 10.

   Depending on the email traffic in your organization, there may be large numbers of users, groups, or domains in the Log Database. This option manages the length of the results list, and the time required to display the search results.
3. Enter 1 or more characters for searching, and then click **Search**.

   Use an asterisk (*) as a wildcard to signify missing characters. For example, J*n might return Jackson, Jan, Jason, Jon, Joan, and so forth.

   Define your search string carefully, to ensure that all desired results are included within the number selected for limiting the search.
4. Highlight 1 or more entries in the results list, and click the right arrow button (>) to move them to the Selected Recipients List.
5. Repeat steps 2 - 4 as needed to conduct additional searches and add more recipients to the Selected Recipients List.
6. To delete an entry from the Selected Recipients List, select the entry and click **Remove**.
7. After you are finished making selections or deletions, click **Next** to open the Message Scanning Results tab.

Selecting message scanning results for the report

The Message Scanning Result tab of the **Presentation Reports > Edit Report** page lets you determine which results of email scanning are included in the report.

Selections are **Clean**, **Virus**, **Spam**, and **Data Security**. By default, all available scanning result types are selected.

Click **Next** to open the Save tab.

Saving the report filter definition

The Save tab of the **Presentation Reports** > **Edit Report** page displays the name and description that will appear in the Report Catalog, and lets you choose how to proceed.

1. Review the Name and Description text.

   If any changes are needed, click **Back** to return to the General tab, where you can make those changes. You cannot edit the name or description text in the Save tab. (See *Setting general report options*, page 114.)
2. Indicate how you want to proceed:
   - Select **Save** to save the report filter and return to the Report Catalog.
   - Select **Save and run** to save the report filter and open the Run Report page. See *Running a presentation report*, page 118.
   - Select **Save and schedule** to save the report filter and open the Scheduler page. See *Scheduling a presentation report*, page 119.
3. Click **Finish** to save the report name and description and implement the selection made in step 2.

Working with Favorites

You can mark any presentation report, either template or custom, as a Favorite. Use this option to identify the reports you generate most frequently and want to be able to locate quickly in the Report Catalog.

To mark a report as a Favorite:

1. On the Presentation Reports page, select a report in the Report Catalog that you generate frequently, or want to be able to locate quickly.
2. Click **Favorite**.

   A star symbol appears beside any Favorite report name in the list, letting you quickly identify it when the Report Catalog is displayed.
3. Mark the **Show Only Favorites** check box above the Report Catalog to limit the list to those marked as Favorites. Clear this check box to restore the full list of reports.

If your needs change and a favorite report is no longer being used as frequently, you can remove the Favorite designation as follows:

1. Select a report that shows the Favorite star symbol.
2. Click **Favorite**.

   The star symbol is removed from that report name in the Report Catalog. The report is now omitted from the list if you choose **Show Only Favorites**.

Running a presentation report

Use the **Presentation Reports > Run Report** page to generate a single report immediately. You can also create jobs with 1 or more reports and schedule them to run once or on a repeating cycle (see *Scheduling a presentation report*, page 119).

> **Note**
>
> Before generating a report in PDF format, make sure that Adobe Reader v7.0 or later is installed on the machine from which you are accessing TRITON - Email Security.
>
> Before generating a report in XLS format, make sure that Microsoft Excel 2003 or later is installed on the machine from which you are accessing TRITON - Email Security.
>
> If the appropriate software is not installed, you have the option to save the file.

To run a report:

1. Select the report you want to run in the Report Catalog and click **Run** to open the Run Report page.
2. Select the **Report start date** and **Report end date** to define the time period covered in the report.
3. Select a **Report output format** for the report.

XLS	Excel spreadsheet. XLS files are formatted for reuse, and can be opened in Microsoft Excel.
PDF	Portable Document Format. PDF files are formatted for viewing, and can be opened in Adobe Reader.
HTML	HyperText Markup Language. HTML files are formatted for viewing, and can be opened in a Web browser.

4. If you selected a Top N report type, choose the number of items to be reported.
5. Specify how you want the report to be generated:
   - Select **Run the report in the background** (default) to have the report run immediately as a scheduled job. Optionally, you can provide an email address to receive a notification message when the report is complete or cannot be generated. (You can also monitor the job queue for report status.)

     If you run the report in the background, a copy of the completed report is automatically saved, and a link to the report appears on the Review Reports page.
   - Deselect **Run the report in the background** to have the report run in the foreground. In this case, the report is not scheduled, and does not appear on the Review Reports page.

If you run the report in the foreground, the report is not automatically saved when you close the application used to view the report (Microsoft Excel, Adobe Reader, or a Web browser, for example). You must save the report manually.

> **Note**
> If you plan to run multiple reports in the foreground, make sure that you use the embedded **Close** button to close the pop-up window used to display the "generating report" and "report complete" messages. If you use the browser's close (X) button, subsequent attempts to run reports in the foreground may fail until you navigate away from the Presentation Reports page, come back, and run the report again.

6. Click **Run**.
   - If you scheduled the report to run immediately, the completed report is added to the Review Reports list. To view, save, or delete the report, click **Review Reports** at the top of the Presentation Reports page.
   - If you ran the report in the foreground, a new browser window appears, displaying report progress. HTML reports appear in the browser window when complete; with PDF or XLS formats, you have a choice of whether to open the report or save it to disk.
7. To print a report, use the print option offered by the application used to display the report.

   For best results, generate PDF output for printing. Then, use the print options in Adobe Reader.

Scheduling a presentation report

You can run presentation reports as they are needed, or you can use the **Presentation Reports > Scheduler** page to create jobs that define a schedule for running 1 or more reports. In an appliance cluster, only the primary machine can schedule a report.

Reports generated by scheduled jobs are distributed to 1 or more recipients via email. As you create scheduled jobs, consider whether your email server will be able to handle the size and quantity of the attached report files.

The completed reports are also added to the **Presentation Reports > Review Reports** page (see *Reviewing scheduled presentation reports*, page 125).

You can access the Scheduler in one of the following ways:

- Click **Scheduler** at the top of the Presentation Reports page (above the Report Catalog).
- When editing a report filter, choose **Save and schedule** in the Save tab, and then click **Finish** (see *Defining the report filter*, page 114).
- Click the job name link on the Job Queue page to edit a job.

- Click **Add Job** on the Job Queue page to create a new job.

The Scheduler page contains several tabs for selecting the reports to run and the schedule for running them. For detailed instructions on completing each tab, see:

- *Setting the schedule*, page 121
- *Selecting reports to schedule*, page 122
- *Setting the date range*, page 122
- *Selecting output options*, page 123

After creating jobs, use the Job Queue to review job status and find other helpful information (see *Viewing the scheduled jobs list*, page 124).

When a scheduled presentation report has run, the report file is sent to recipients as an email attachment. The name of the attachment is the report name. For example, for a report with an output format of PDF, an attachment file may be named Hybrid Service Messages.pdf.

Scheduled reports are also automatically saved to a report output directory on the TRITON - Email Security machine (C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\temp\report\output, by default). Note that the name of the attachment sent via email does not match the name of the file stored in the output directory. The best way to find a specific report is to use the Review Reports page, which can be searched by date or job name, as well as report name.

Reports are automatically deleted from the Review Reports page and the report output directory after the period specified on the **Settings** > **Reporting** > **Preferences** page (5 days, by default). If you want to retain the reports for a longer time, include them in your backup routine or save them in a location that permits long-term storage.

An alert is displayed on the Review Reports page for a period of time before the report is deleted (3 days, by default). Use the **Settings** > **Reporting** > **Preferences** page to change this warning period.

Depending on the number of reports you generate daily, report files can occupy considerable amounts of disk space. Be sure adequate disk space is available on the TRITON - Email Security machine. If the report output directory grows too large before the files are automatically deleted, you can delete the files manually.

Websense software generates the report in the format you choose: XLS (Microsoft Excel), PDF (Adobe Reader), or HTML. If you choose HTML format, the report may display in the TRITON - Email Security content pane. Reports displayed in the

content pane cannot be printed or saved to a file. To print or save a report to file, choose the PDF or XLS output format.

> **Important**
>
> To display presentation reports in PDF format, Adobe Reader v7.0 or later must be installed on the machine from which you are accessing TRITON - Email Security.
>
> To display presentation reports in XLS format, Microsoft Excel 2003 or later must be installed on the machine from which you are accessing TRITON - Email Security.

Setting the schedule

Schedule a reporting job to occur once or on a repeating cycle on the Schedule Report tab of the **Presentation Reports > Scheduler** page.

> **Note**
>
> It is advisable to schedule report jobs on different days or at different times, to avoid overloading the Log Database and slowing performance for logging and interactive reporting.

1. Enter a name that uniquely identifies this scheduled job in the **Job name** field.
2. Select Recurrence Options for the job based on the Recurrence Pattern you want, as follows:

Recurrence Pattern	Recurrence Options
Once	Enter the exact date on which to run the job, or click the icon to select from a calendar.
Daily	No additional recurrence options are available.
Weekly	Mark the check box for each day of the week the job is to run.
Monthly	Enter the dates during the month for running the job. Dates must be a number between 1 and 31, and must be separated by commas (1,10,20). To run the job on consecutive dates each month, enter a start and end date separated by a hyphen (3-5).

3. In the Schedule Time box, set the start time for running the job.

   The job begins according to the time on the machine running TRITON - Email Security.

> **Note**
>
> To start generating the scheduled reports today, select a time late enough that you can complete the job definition before the start time.

4. In the Schedule Period box, select a date for starting the job. Options for ending the job are as follows:

No end date	The job continues to run indefinitely, according to the established schedule. To discontinue the job at some time in the future, either edit or delete the job. See *Viewing the scheduled jobs list*, page 124.
End after	Select the number of times to run the job. After that number of occurrences, the job does not run again, but it stays in the Job Queue until you delete it. See *Viewing the scheduled jobs list*, page 124.
End by	Set the date when the job stops running. It does not run on or after this date.

5. Click **Next** to open the Select Report tab.

Selecting reports to schedule

Use the Select Report tab of the **Presentation Reports > Scheduler** page to choose reports for the job.

1. Highlight a report for this job in the Report Catalog tree.
2. Click the right arrow (>) button to move that report to the Selected Reports list.
3. Repeat steps 1 and 2 until all reports for this job appear in the Selected Reports list.
4. Click **Next** to open the Date Range tab.

Setting the date range

Use the Date Range tab of the **Presentation Reports > Scheduler** page to set the date range for the job. The options available depend on your selection for date range.

All Dates	Reports include all dates available in the Log Database. No additional entries are required. When this option is used for repeating jobs, duplicate information may appear on reports in separate runs.

Specific Dates	Choose the exact start (From) and end (To) dates for the reports in this job. This option is ideal for jobs that run only 1 time. Choosing this option for a repeating schedule results in duplicate reports.
Relative Dates	Use the drop-down lists to choose the number of periods to report (Current, Last, Last 2, and so forth), and the type of period (Days, Weeks, or Months). For example, the job might cover the Last 2 Weeks or Current Month. Week represents a calendar week, Sunday through Saturday. Month represents a calendar month. For example, Current Week produces a report from Sunday through today; This Month produces a report from the first of the month through today; Last Week produces a report for the preceding Sunday through Saturday; and so forth. This option is ideal for jobs that run on a repeating schedule. It lets you manage how much data appears on each report, and minimize duplication of data on reports in separate runs.

After setting the date range for the job, click **Next** to display the Output tab.

Selecting output options

After you select the reports for a job, use the Output tab to select the output format and distribution options.

1. Select the file format for the finished report.

XLS	Excel Spreadsheet. Recipients must have Microsoft Excel 2003 or later to view the XLS reports.
PDF	Portable Document Format. Recipients must have Adobe Reader v7.0 or later to view the PDF reports.
HTML	HyperText Markup Language. Recipients must have a Web browser.

2. Select the number of items you want to appear in a Top format report from the **Top N** drop-down list. The value range is from 1 to 200; default value is 10.
3. Enter recipient email addresses for report distribution.

   Each address should be separated by a semicolon.
4. Optionally, you can also enter email addresses to notify recipients that report generation failed.
5. Mark the **Customize subject and message body of notification email** check box, if desired. Then, enter the custom subject and body text for this job's distribution email.
6. Click **Save Job** to save and implement the job definition, and display the Job Queue page.
7. Review this job and any other scheduled jobs. See *Viewing the scheduled jobs list*, page 124.

Viewing the scheduled jobs list

The **Presentation Reports** > **Job Queue** page lists the scheduled jobs created for presentation reports. The list gives the status for each job, as well as basic information about the job, such as how frequently it runs. From this page, you can add and delete scheduled jobs, temporarily suspend a job, and more.

You can search for a particular job by entering a search term in the **Job name** entry field at the top of the page. Click **Go** to begin the search.

Click **Clear** to remove the current search term, and then either perform a different search or click **Refresh** at the bottom of the page to display the complete list of reports.

The list provides the following information for each job:

Data Item	Description
Job Name	The name assigned when the job was created.
Status	Indicates whether the job is • running • scheduled (waiting for the next scheduled run time) • completed successfully • failed • misfired (did not run at the last scheduled time due to a problem such as low memory or server shutdown)
State	One of the following: • **Enabled** indicates a job that runs according to the established recurrence pattern. • **Disabled** indicates a job that is inactive, and does not run.
Recurrence	The recurrence pattern (Once, Daily, Weekly, or Monthly) set for this job.
History	Click the Details link to open the Job History page for the selected job. See *Viewing job history*, page 125.
Next Scheduled	Date and time for the next run.
Owner	The user name of the administrator who scheduled the job.

Use the options on the Job Queue page to manage the jobs. Some of the buttons require that you first mark the check box beside the name of each job to be included.

Action	Description
Job name link	Opens the Scheduler page, where you can edit the job definition. See *Scheduling a presentation report*, page 119.
Run Now	Starts running any job that has been selected in the list immediately. This is in addition to regularly scheduled job runs.
Add Job	Opens the Scheduler page where you can define a new job. See *Scheduling a presentation report*, page 119.

Action	Description
Delete	Deletes from the Job Queue any job that has been selected in the list. After a job has been deleted, it cannot be restored. To temporarily stop running a particular job, use the **Disable** button.
Enable	Reactivates a disabled job that has been selected in the list. The job begins running according to the established schedule.
Disable	Discontinues running an enabled job that is selected in the list. Use this option to temporarily suspend a job that you may want to restore in the future.
Refresh	Updates the page with the latest data

Viewing job history

Click the **Details** link in the History column and use the **Presentation Reports** > **Job Queue** > **Job History** page to view information about recent attempts to run the selected job. The page lists each report separately, providing the following information:

Data Item	Description
Report Name	Title printed on the report
Start Date	Date and time the report started running
End Date	Date and time the report was completed
Status	Indicator of whether the report completed or failed
Message	Relevant information about the job, such as whether the report was successfully distributed

Reviewing scheduled presentation reports

Use the **Presentation Reports** > **Review Reports** page to find, access, and delete scheduled reports. By default, reports are listed from newest to oldest.

To view any report in the list, click the report name.

- If the report is a single PDF or XLS file, you may be given the option to save or open the report. This depends on your browser security settings and the plug-ins installed on your machine.
- If the report is very large, it may have been saved as multiple PDF or XLS files and stored in a ZIP file. The file is compressed using ZIP format. Save the ZIP file, then extract the PDF or XLS files it contains to view the report content.
- Hover the mouse pointer over the report icon next to the report name to see if the report is 1 or multiple files.

To limit the list to reports that will be deleted soon, mark the **Show only reports due to be purged** check box. The length of time that reports are stored is configured on the **Settings** > **Reporting** > **Preferences** page (see *Configuring reporting preferences*, page 111).

To search the report list, first select an entry from the **Filter by** drop-down list, and then enter all or part of a job name or date. Note that the search is case-sensitive. You can search by:

- The report or job name
- The date the report was created (Creation Date)
- The name of the administrator that scheduled the report (Requestor)
- The date the report is due to be deleted (Purge Date)

Click **Go** to begin the search.

Click **Clear** to remove the current search term, and then either perform a different search or click **Refresh** to display the complete list of reports.

If a recently completed report does not appear on the Review Reports page, you can also click **Refresh** to update the page with the latest data.

To delete a report, mark the check box beside the report name and click **Delete**.

To see the status of a scheduled report job, click **Job Queue** at the top of the page. See *Viewing the scheduled jobs list*, page 124, for more information about using the job queue.

To schedule a new report job, click **Scheduler** (see *Scheduling a presentation report*, page 119).

7 Configuring Personal Email Manager End User Options

Personal Email Manager enables users to review personal lists of quarantined email messages and decide whether to delete the messages or treat them as legitimate email and deliver them. This facility also allows a user to manage personal Always Block and Always Permit email address lists and delegate blocked email management to at least 1 other individual.

Use the **Settings > Personal Email** page of Email Security Gateway to set up the Personal Email Manager environment for your end users. Import a Secure Sockets Layer (SSL) certificate for Personal Email Manager communications. Configure the notification message that tells users mail sent to them has been blocked. Authorize an end user to manage personal Always Block and Always Permit lists, enable some user account management functions, and configure the appearance of the Personal Email Manager end-user display.

You can also identify the IP address of the appliance on which an end user can access Personal Email Manager. Personal Email Manager users must have Personal Email Authentication permissions in order to use the facility. See *Managing user validation/authentication options*, page 54, for information about granting Personal Email Manager permissions to end users.

Topics:

Managing a Secure Sockets Layer (SSL) certificate

Use the **Settings > Personal Email > SSL Certificate** page to manage the Personal Email Manager SSL certificate, which enables secure email transmission for Personal Email Manager appliances. You can use the default certificate provided with Personal Email Manager, or you can import a new enterprise certificate from a certificate authority (CA).

After Email Security Gateway installation, default certificate information appears in the **Settings** > **Personal Email** > **SSL Certificate** page, in the Certificate Details section. Details include the certificate version, serial number, issuer, and expiration date.

Importing a certificate

Importing an SSL certificate to Personal Email Manager from a CA replaces the current certificate. Personal Email Manager certificate information is automatically copied to a new appliance when it is added to the Email Security Gateway management server.

Use the following procedure to import a certificate:

1. Click **Import** in the **Settings** > **Personal Email** > **SSL Certificate** page, below the Certificate Details area.
2. Click **Yes** in the confirmation dialog box. An Import Certificate area appears below the Import button.
3. Enter the certificate filename in the **Import Certificate** field or navigate to it using **Browse**. File format must be .jks, .p12, or .pfx.
4. An SSL certificate file should be password protected. Enter a password in the **Certificate password** field (maximum length is 100 characters).
5. Mark the **Private key alias** check box and enter an optional alias (or identifier) for the private key in the entry field.
6. Mark the **Private key password** field and enter an optional password for the private key in the entry field (maximum length is 100 characters).
7. Click **OK**.
8. Restart the Personal Email Manager service to activate the new certificate.

Restoring the default certificate

You can restore the Personal Email Manager default certificate at any time by clicking **Restore Default Certificate** in the **Settings** > **Personal Email** > **SSL Certificate** page. This action replaces the current certificate.

You should restart the Personal Email Manager service to activate the new certificate.

Creating the quarantine mail notification message

The **Settings** > **Personal Email** > **Notification Message** page is composed of 4 sections:

- Notification Message Links, in which you specify the IP address and port for Personal Email Manager facility end-user access (see *Specifying Personal Email Manager access*, page 129)

- Notification Message Schedule, where you set the frequency with which a message is sent informing a user of blocked messages (see *Scheduling the notification message*, page 129)
- Notification Message Template, in which you format the content and appearance of the notification message. Users see this message in their inbox when they have blocked email. (See *Using the notification message template*, page 130.)
- Recipients List, in which you designate the user directories whose members will receive notification messages. (See *Creating the notification message recipient list*, page 131.)

After you complete all 4 sections, click **OK** to enable the delivery of notification messages.

Specifying Personal Email Manager access

Use the Notification Message Links section to designate the appliance that the end user accesses to manage blocked email in the Personal Email Manager tool. This setting is also used to create the hyperlinks to blocked mail listed in the user notification message.

Enter the IP address or host name of the Personal Email Manager appliance.

Enter the port number (default is 9449). The port number should not be an Email Security Gateway or appliance reserved port.

> **Note**
> If you use the C appliance interface for Personal Email Manager access, you must use the default port of 9449.

Deploy a group of Email Security appliances to handle Personal Email Manager end-user activities. Configuring an appliance cluster for Personal Email Manager access can enhance performance by activating an appliance load-balancing feature. If the appliance you access is configured in a cluster, the appliance forwards Personal Email Manager access requests to other cluster machines using a round robin mechanism.

Add and remove appliances from a cluster using the **Settings** > **General** > **Cluster Mode** page (see *Configuring an appliance cluster*, page 44, for information).

Scheduling the notification message

You have several options for scheduling the frequency of the notification messages that tell users that they have blocked messages. Configure the schedule settings in **Settings** > **Personal Email** > **Notification Message**.

Select the frequency of notification messages in the **Send notifications** drop-down list. By default, **None** is selected, and no other option in this section is enabled.

- If you select **Every day** in the **Send notifications** drop-down list, the **Time** options are enabled for selection. You can choose as many time intervals as you like, in 1-hour increments.
- If you select **Every workday** in the **Send notifications** drop-down list, the **Time** options are enabled for selection. You can choose as many time intervals as you like, in 1-hour increments.
- If you select **Every week** in the **Send notifications** drop-down list, the **Day of week** and **Time** fields are activated. Designate a day of the week for notification messages to be sent. You can choose as many time intervals as you like, in 1-hour increments.

> **Note**
> Notification messages will be sent only to protected domains. Unprotected domains will not receive notification messages.

Using the notification message template

The notification message template helps you determine the content and appearance of the email that informs users of blocked messages. Configure the notification message as follows:

1. Set the maximum number of messages that are included in each notification message. The default value is 50, maximum value is 100. A user with more than the maximum number of blocked messages waiting must handle the excess directly in the Personal Email Manager facility, via the Web Access link in the notification message.
2. Select the email actions you want the notification to include from among the following options:
   - **Not Spam** (default selection), to allow the user to report a blocked message that should not be classified as spam
   - **Deliver** (default selection), to allow the user to have a blocked message delivered
   - **Delete** (default selection), to remove a blocked message from the user's blocked message list
   - **Add to Always Block list**, to allow an authorized user to add an address to a personal Always Block List
   - **Add to Always Permit list**, to allow an authorized user to add an address to a personal Always Permit List
3. Enter your company name and other relevant information in the **Company** entry field.
4. Enter a brief description of the email filtering product in the **Description** entry field (default is "Websense Email Security Gateway").
5. Enter the sender email address for the notification message in the **Sender** field.

6. Configure the subject line that you want the notification message to display in the **Subject** field. This subject will appear in the user's inbox when the notification message is received.
7. Designate some appropriate header text for the notification message in the **Header** field. Default is "The following messages are isolated."
8. Enter some appropriate footer text for the notification message in the **Footer** field. Default is "For more information, contact your administrator."

Creating the notification message recipient list

You can determine which Personal Email Manager users receive notification messages by entering their details into the Recipients List section. Only the users listed in the Recipients list receive notification messages alerting them about blocked email.

The Recipients list is based on user directories. All existing user directories are listed in the left-hand user directories box. Select a user directory and click the right arrow to add the directory to the **Recipients** list.

Click **Add user directory** to create a new directory on the Add User Directory page (see *Adding and configuring a user directory*, page 46, for details). After you create a new user directory, it will appear in the user directories list on the Notification Message page.

If you want to delete a user directory from the Recipients list, select the directory in the Recipients list and click **Delete**.

Setting user account options

You can configure some Personal Email Manager user account options in the **Settings > Personal Email > User Accounts** page. Allow users to manage personal Always Block and Always Permit lists, delegate blocked message management to another individual, and manage multiple user accounts in a single Personal Email Manager session.

Authorizing use of block and permit lists

Authorized users can manage their own Always Block and Always Permit lists after they log in to Personal Email Manager. Use the **Settings** > **Personal Email > User Accounts** page to specify users who can manage entries in personal block and permit lists.

Adding authorized users

You can allow users to manage personal Always Block and Always Permit lists by specifying user directories that contain users with Personal Email Manager authentication privileges. Create user directories (in the User Directories page), and

then specify authentication options for these user directories in the Add User Authentication page. (See *Adding and configuring a user directory*, page 46, for user directory details and *Managing user validation/authentication options*, page 54, for information about user authentication settings.)

In the **Settings > Personal Email > User Accounts** page, user directories for which you have specified Personal Email Manager privileges appear as available user directories. To grant permission for a user directory group to manage personal block/permit lists, select a user directory in the available directories list by marking the check box next to the directory name, and click the arrow button to move it to the Recipients box.

Removing authorized users

Remove previously authorized users by selecting a user directory in the Recipients box and clicking **Delete**. The user directory still appears in the available directories box, but its members no longer have Always Block/Always Permit list management permissions.

Enabling user account management

You can enable the following user account management functions for a Personal Email Manager end user by marking the **Enable user account management** check box in the **Settings > Personal Email > User Accounts** page:

- Allow an end user in a non-LDAP based user directory to manage multiple Personal Email Manager email accounts in the same session.

  Note
  For Personal Email Manager users in LDAP-based user directories, this function can be enabled on the Add or Edit User Directory page by marking the **Enable multiple user email account access in a single Personal Email Manager session** check box. See *Managing user directories*, page 46, for details.

- Let an end user delegate the management of blocked messages to 1 or more other individuals.

End users can configure these options in the User Account Access page, in the Personal Email Manager end-user interface. See *Personal Email Manager User Help* for details.

Customizing the Personal Email Manager end-user portal

You can use the **Settings > Personal Email > End-user Portal** page to customize the end-user facility's appearance and to designate the quarantined message queues whose messages are displayed in Personal Email Manager end-user notification email.

Choosing a logo display

By default, the Websense company name and logo appear on the Personal Email Manager end-user page. You may choose to have no company name or logo appear on the portal. For this option, leave the Company name field blank and select **None** in the Logo field drop-down list.

You can also customize the end-user portal by having your company name and logo appear there. Use the following procedures to customize your Personal Email Manager end-user portal in the End-user Portal Options section:

1. Enter your company name in the **Company name** field.
2. In the Logo field drop-down list, select **Custom**.
3. The **Upload logo** field appears. Browse to your logo file and select it for upload. The logo file must be:
   - A .gif, .png, .jpeg, or .jpg file format
   - Up to 1 MB and 120 x 34 pixels in size

You can change the logo file you use by clicking **Browse** next to your logo filename and browsing to a new logo file.

Choosing quarantine message queue display

Select the queues whose messages are displayed to Personal Email Manager end users by marking the check box next to the desired queue name in the Message Queue Display Settings section.

Index

A

D

E

F

G

H

I

L

M

N

P

S

T

U

V

W