



Installation Guide

WebSense Email Security

©Copyright 2004-2009 Websense, Inc. All rights reserved.

All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
Published 2009

Printed in the United States of America and Ireland.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

Websense, the Websense Logo, Threatseeker and the YES! Logo are registered trademarks of Websense, Inc. in the United States and/or other countries. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

This product includes the following:

ActiveMQ version 2.1

Copyright © 2009 The Apache Foundation

ADAPTIVE Communication Environment version 5.6.5

This product includes ADAPTIVE Communication Environment, which is copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University,

Copyright (c) 1993-2008, all rights reserved.

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

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

The Apache Software License, Version 2.0

This product includes the Xerces-C software developed by the Apache Software Foundation (<http://www.apache.org/>)

Copyright © 2009 The Apache Software Foundation. All Rights Reserved.

The following LICENSE file terms are associated with the XERCES-C-SRC_2_6_0 code of E-mail Filter for SMTP

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

END OF TERMS AND CONDITIONS

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

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

Copyright [yyyy] [name of copyright owner]

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

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

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

bzip2 version 1.0.2

Copyright © 1996 - 2009 julian@bzip.org

Compression Plus version 5.0.1.27

Copyright © 1992 - 2003 BeCubed Software, Inc.

GoAhead Software version 2.1

Copyright © 2009 GoAhead Software, Inc.

gSOAP version 2.7.10

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright ©2001-2009 Robert A. van Engelen, Genivia inc. All Rights Reserved.

ICU License - ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2009 International Business Machines Corporation and others. 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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

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

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

Jacob version 1.14.3

Copyright © 1991, 1999 Free Software Foundation, Inc.

Java Native Interface

Copyright 1994-2009 Sun Microsystems, Inc. All Rights Reserved.

Java Runtime Environment version 6.0.0.105

Copyright 1994-2009 Sun Microsystems, Inc. All Rights Reserved.

JBoss version 4.0.3 SP1

Copyright © 2007 Free Software Foundation, Inc.

jRegistryKey version 1.4.4

Copyright © 2007 Free Software Foundation, Inc.

jTDS version 1.2.3

Copyright © 2007 Free Software Foundation, Inc.

Launch4j version 3.0.1

Copyright © 2004, 2008 Grzegorz Kowal

Log4j version 1.2.15

Copyright © 2009 The Apache Foundation

OpenSSL

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

Copyright © 1998-2009 The OpenSSL Project. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

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

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

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

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

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

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

POSSIBILITY OF SUCH DAMAGE.

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

RSA MD5 by RSA Data Security (Open Source)

Portions of this product contain or are derived from:

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm.

MDDRIVER.C - test driver for MD2, MD4 and MD5

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

UNRAR version 3.50.0.214

Copyright © 2007 Free Software Foundation, Inc.

zlib version 1.2.3

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

This notice may not be removed or altered from any source distribution.

Contents

Chapter 1	Preparing to Install.	9
	System requirements	9
	Windows Server and SQL Server 2008	10
	File sharing.	11
	SQL Server passwords.	11
	SQL Server connection	11
	Personal Email Manager and Report Central	12
	Other requirements	13
	Pre-installation considerations	13
	Inbound and outbound filtering.	13
	Database considerations	14
	SQL Server or SQL Server 2005 Express	14
	Dedicated or centralized	14
	Database size	14
	SQL Server behind a firewall	15
	Load balancing methods	15
	Server size	17
	Deployment recommendations.	18
	Dedicated Websense Email Security deployment.	19
	Inbound connections	19
	Outbound connections	20
	Firewall configuration	20
	Websense Email Security deployment in a DMZ.	21
	Database connections.	21
	Inbound connections	21
	Outbound connections	22
	Relaying email	22
	Multiple Websense Email Security servers.	22
	Multiple servers deployed for redundancy	22
	Multiple servers with centralized databases	25
	Installing on Windows 2000	27
	Preparing to import users and groups (optional)	27
	Implementing rules using these users and groups.	28
Chapter 2	Installation.	29
	Installation options	29
	Configuration after installation.	29
	Upgrading from earlier versions.	30

Upgrading the server	30
Upgrading the client	31
Possible upgrade interruption	31
Installing Websense Email Security	31
Websense Email Security Setup Wizard	32
Websense Email Security Configuration Wizard	35
Installing the Administration Client	39
Rolling back to your previous version	41

1

Preparing to Install

Websense Email Security allows you to filter and manage your organization's email and enforce an Acceptable Use Policy (AUP). This process reduces risks to productivity, network resources, legal liability, and security from improper use of email.

System requirements

The following table lists the system requirements for the machine running Websense Email Security server components.

Server minimum requirements

Component	Requirement
Processor	Intel Pentium IV processor 1.4 GHz or higher, minimum Intel Pentium D 3.0 GHz or higher, recommended
Memory	2 GB RAM minimum, 4 GB recommended
Operating System	Windows 2000 Server Service Pack 4 Windows Advanced Server 2000 Service Pack 4 Windows Server 2003 Service Pack 2 (Standard or Enterprise Edition) Windows Server 2003 R2 Enterprise Edition Service Pack 2 Windows Server 2003 R2 x64 Enterprise Edition Service Pack 2 Windows Server 2008 Service Pack 2 (Standard or Enterprise Edition) Windows Server 2008 x64 Service Pack 2 (Standard or Enterprise Edition)
Disk Space	15 GB minimum, 20 GB recommended
Display	Super VGA (800 x 600) or higher resolution video adapter and monitor
Web Browser	Microsoft Internet Explorer 6.0 SP1 or later Mozilla Firefox 2.0 or later
Networking	TCP/IP installed and configured with an Internet connection
DNS	Internal or external DNS configured
Email	Email system with SMTP gateway or MTA installed

Server minimum requirements (Continued)

Component	Requirement
MDAC	Microsoft Data Access Components MDAC 2.8 (Service Pack 1) or later
Database	<p>Microsoft SQL Server 2000 Service Pack 4</p> <p>Microsoft SQL Server 2005 Service Pack 2 (Workgroup, Standard, or Enterprise)</p> <p>Microsoft SQL Server 2005 Express Service Pack 2 or Service Pack 3</p> <p>Microsoft SQL Server 2008 Enterprise Edition Service Pack 1</p> <p>Websense Email Security uses a relational database to store rules, system configuration, and dictionaries.</p> <p>If SQL Server is not installed on your system, Websense Email Security can install SQL Server 2005 Express SP2, or you can use a database engine on another machine.</p> <p>The full SQL Server is recommended for larger sites, because it handles large volumes of data more easily.</p>

The following table lists the system requirements for the machine running Websense Email Security administration client components.

Separate administration client minimum requirements

Component	Requirement
Processor	Pentium IV, 1.4 GHz or higher
Disk Space	100 MB minimum, 300 MB recommended
Operating System	<p>Windows 2000 Server Service Pack 4</p> <p>Windows 2000 Professional Service Pack 4</p> <p>Windows Advanced Server 2000 Service Pack 4</p> <p>Windows Server 2003 Standard Edition Service Pack 2</p> <p>Windows Server 2003 Enterprise Edition Service Pack 2</p> <p>Windows Server 2003 R2 Enterprise Edition Service Pack 2</p> <p>Windows Server 2003 R2 x64 Enterprise Edition Service Pack 2</p> <p>Windows XP Professional Service Pack 2</p> <p>Windows Vista Service Pack 1</p>
Display	Super VGA (800 x 600) or higher resolution video adapter and monitor
Web Browser	<p>Microsoft Internet Explorer 6.0 SP1 or later</p> <p>Mozilla Firefox 2.0 or later</p>
MDAC	Microsoft Data Access Components MDAC 2.8 (Service Pack 1) or later

Windows Server and SQL Server 2008

If your operating system is Windows Server 2008 or your database uses SQL Server 2008, you need to modify some system settings for Websense Email Security to run properly.

File sharing

Windows Server 2008 supports 2 types of file sharing: public file sharing and standard file sharing. Both types of file sharing must be enabled for Websense Email Security to function properly in a cluster configuration running Windows Server 2008.

File sharing is controlled in the Windows Network and Sharing Center. You can enable file sharing as follows:

1. Navigate to the Network and Sharing Center window, which lists file sharing options (**Start > Control Panel > Network and Sharing Center**).
2. In the Sharing and Discovery section, click the down arrow to the right of the **File sharing** option and choose to enable standard file sharing.
3. In the Sharing and Discovery section, click the down arrow to the right of the **Network discovery** option and choose to enable network discovery.

SQL Server passwords

Password requirements under Windows Server 2008 are more complex than those for earlier versions. If you are running Windows Server 2008, the password must

- ◆ Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- ◆ Be at least six characters in length
- ◆ Contain characters from three of the following four categories:
 - Uppercase characters (A – Z)
 - Lowercase characters (a – z)
 - Digits (0 – 9)
 - Special keyboard characters (for example, !, \$, #, %, @)

If you use SQL Server versions prior to 2008 with Windows Server 2008, SQL Server passwords must adhere to these guidelines.

SQL Server connection

Security features in Windows Server 2008 require additional settings for local and remote connection to SQL Server 2008.

For a connection to a local instance of SQL Server 2008, you must add localhost to your Internet trusted sites:

1. Open the Internet Options dialog box (**Tools > Internet Options**) and select the Security tab.
2. Select the Trusted Sites zone and click **Sites**.
3. Add http://localhost in the **Trusted sites** dialog box.
4. Click **Add** and then **Close**.
5. Click **OK**.

In addition to making localhost a trusted Internet site, you must modify settings in the SQL Server Configuration Manager for a connection to a remote SQL Server 2008, as follows:

1. Open the SQL Server Configuration Manager from the Start menu (**Start > All Programs > Microsoft SQL Server 2008 > SQL Server Configuration Manager**). You can also right-click My Computer and select **Manage**. In Computer Management, expand **Services and Applications**.
2. Expand **SQL Server Configuration Manager**.
3. Expand **SQL Server Network Configuration** and select **Client Protocols**.
4. In the list of protocols, right-click the **TCP/IP** protocol and then click **Enable**.
5. Right-click the **Named Pipes** protocol and then click **Enable**.

You also need to add security policies to allow a remote connection to SQL Server 2008. Refer to [SQL Server behind a firewall](#) for more information.

Personal Email Manager and Report Central

Websense Email Security v7.2 is compatible with:

- ◆ Personal Email Manager version 7.2
All Personal Email Manager features are supported.
- ◆ Report Central version 2.7.2
Status information for Report Central version 2.7.2 appears on the Dashboard in Websense Email Security.
No Report Central status information appears on the Dashboard if you integrate with a Report Central version earlier than 2.7.2.

Install Websense Email Security before installing Personal Email Manager on a separate computer. Websense Email Security and Personal Email Manager need to be installed on separate computers in most installations.

In small networks of 250 users or fewer, Websense Email Security, Personal Email Manager, and Report Central may be installed on one machine, depending on email volume. See the *Personal Email Manager Installation Guide* for system requirements when installing Websense Email Security and Personal Email Manager on the same machine.

You should upgrade Personal Email Manager and Report Central when you upgrade Websense Email Security. Installers and installation instructions for these modules are provided with the Websense Email Security version 7.2 product. By default, they are located in the folder to which Websense Email Security is extracted (C:\Websense).

Other requirements

- ◆ Full administrative rights on the installation machine
- ◆ Windows Installer 3.1 and .NET Framework 2.0 or later (only if you plan to install SQL Server 2005 Express)
- ◆ Before beginning the installation, gather the following information:
 - Email system's pre-registered domain name
 - IP address or host name of your email system's SMTP gateway or MTA
 - Email address of the email administrator
 - Subscription key from Websense, Inc. (available from www.websense.com/MyInfo)
 - Available HTTP port number (default 8181) to install and start the Administration service
 - Available HTTP port number 9090 to install and start the Dashboard service
 - IP address of the relay host (for example your ISP), if you are not using Mail Exchanger (MX) records

Pre-installation considerations

Consider the following options as you plan your installation.

- ◆ Both inbound and outbound filtering?
- ◆ Which database management system?
- ◆ Database location?
- ◆ Database size?
- ◆ Load balancing methods?
- ◆ Server size?

Inbound and outbound filtering

Websense Email Security stops spam at the gateway, which reduces the load on network resources. If your main focus is to stop spam and other unwanted content from entering your network, configure Websense Email Security for inbound filtering only.

Websense Email Security provides significant additional benefits if you configure it to perform outbound filtering. Outbound filtering can scan for confidential or potentially damaging information before routing the email to the intended recipient. Outbound filtering can also be used to add company footers, enforce TLS encryption, and for tracking email usage in your network.

Threat-prevention policies can apply to both inbound and outbound traffic. For example, a single policy can stop inbound and outbound viruses.

Database considerations

Websense Email Security creates the following databases in Microsoft SQL Server:

- ◆ STEMConfig – Stores all configuration data and filtering policies
- ◆ STEMLog – Stores all logging data; the default size of this database is 1.5 GB.
- ◆ STEMFriendlyName – Stores the details of the friendly name aliases of email addresses
- ◆ STEMDashboard – Stores data collected from the different Websense Email Security services to display on the Dashboard, along with Dashboard configuration data

SQL Server or SQL Server 2005 Express

If no database is detected during installation, you have the option to use an instance of SQL Server on a different machine, or to install Microsoft SQL Server 2005 Express SP2. SQL Server Express is a free, runtime version of Microsoft SQL Server. Its database capacity is 4 GB.

Although you can install a SQL Server database onto the Websense Email Security server, Websense, Inc., recommends that large environments install a licensed version of the full SQL Server on a separate, dedicated server.

Dedicated or centralized

Some organizations require multiple Websense Email Security servers, either because there are multiple email server hosts, or to process their large email volume more quickly.

In this deployment, there are two database options: dedicated or centralized.

- ◆ Dedicated – Data for a single Websense Email Security server resides in its own, separate database.
- ◆ Centralized – Data for multiple Websense Email Security servers resides in a single, centralized database.

A centralized database option offers centralized policy management and message administration, plus reports from a single repository.

However, a centralized database grows in relation to the number of Websense Email Security servers writing to it, and may require additional administration.

If you choose a centralized database, see [Multiple Websense Email Security servers](#), page 22, for additional configuration and management information.

Database size

The size of the database correlates to the number of email messages your organization receives per day, and to the length of time you plan to retain the logged data for message administration and reporting. Other factors include the average number of

recipients per message, and the specific processing required to implement your organization's policy.

To estimate the size your database, note that each email generates approximately 1 KB to 5 KB of log data. For example, 1 GB is the minimum disk space required for 1 million messages.

The server storing the Websense Email Security data must have enough RAM to accommodate the anticipated size of the database. For example, the Microsoft recommendation for optimal performance indicates that a 1 GB database requires 1 GB of RAM.

SQL Server behind a firewall

If SQL Server resides in the DMZ, and Websense Email Security resides inside the network, you must configure a tunnel on the firewall for the appropriate ports.

- ◆ If SQL Server is the default instance: TCP/IP port 1433 (default)
- ◆ If SQL Server is a named instance: TCP/IP port assigned to that instance, and UDP port 1434
- ◆ If SQL Server listens over named pipes: UDP ports 445 and 139

For additional information, consult the following Microsoft knowledge base articles:

- ◆ TCP Ports Needed for Communication to SQL Server Through a Firewall
<http://support.microsoft.com/kb/287932>
- ◆ How To Use ADO to Connect to a SQL Server That Is Behind a Firewall
<http://support.microsoft.com/kb/269882/EN-US/>

Load balancing methods

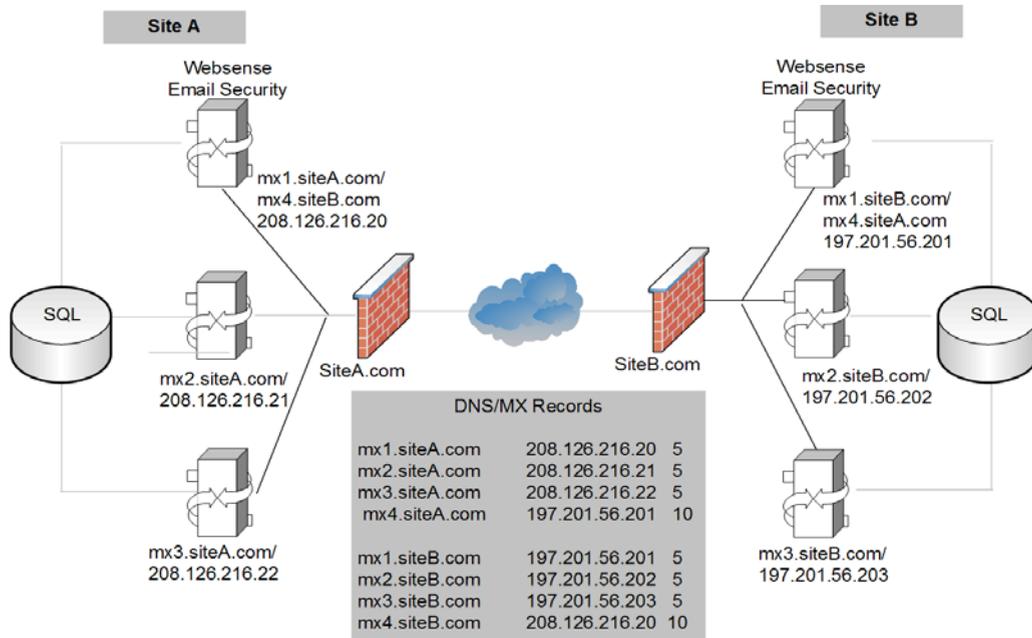
You can load balance Websense Email Security using Mail Exchanger (MX) records. On the DNS server hosting your domain, create an MX record for each primary Websense Email Security server using the same MX preference, while giving the failover server a higher preference number (which gives it a lower preference). The following table provides an example of MX preference assignments for load balancing and failover using MX records.

MX records for load balancing		
Mail exchanger	IP Address	MX Preference
Site A		
mx1.siteA.com	208.126.216.20	5
mx2.siteA.com	208.126.216.21	5
mx3.siteA.com	208.126.216.22	5
mx4.siteA.com	197.201.56.201	10
Site B		
mx1.siteB.com	197.201.56.201	5

MX records for load balancing

Mail exchanger	IP Address	MX Preference
mx2.siteB.com	197.201.56.202	5
mx3.siteB.com	197.201.56.203	5
mx4.siteB.com	208.126.216.20	10

The following figure illustrates this example:



Using MX records for load balancing

In the preceding diagram, email sent to siteA.com round-robins between mail exchangers 1, 2, and 3, because each Websense Email Security server has the same MX preference of 5. A lower MX preference number means that it has a higher priority. For example, 5 has a higher priority than 10.

The same round-robin occurs for email messages sent to siteB.com.

If site A is unavailable, the sending mail server routes email to the fourth (failover) MX record, which is the address of a server at siteB.com.

For the failover to work properly, Websense Email Security servers in site A are configured to accept messages for site B, and Websense Email Security servers in site B are configured to accept messages for site A. The failover servers also have static routes configured so that Websense Email Security knows where to route the email.

In addition to using MX records for load balancing and failover, you can use load balancing switches. These switches offer a variety of load balancing algorithms and round-robin delivery, to provide efficient load distribution and timely failover. Load

balancing switches can improve the overall efficiency of your SMTP infrastructure, but they are not required.

Server size

Websense Email Security requires Windows Server 2000 SP4 or greater, Windows Server 2003 SP2 or greater, or Windows Server 2008 SP1. If you are using Windows Server 2000 SP4, the Advanced Server edition is recommended for high-volume email environments.

The following table shows minimum recommendations for the Websense Email Security server, according to the number of email messages per hour that your organization handles.

Keep in mind that the specific requirements for each organization depend on several factors: number of rules processing threads, number of enabled rules, size of email messages, and complexity of email messages (such as attachments and embedded files).

Minimum server recommendations	
Email messages per hour	Minimum server recommendations
< 10,000	Pentium 4, 1.4 GHz, 1 GB RAM
< 25,000	Dual Xeon, 2 GB RAM
< 40,000	Quad Xeon, 2 GB RAM, 3 or more hard drives (10,000+ RPM) for email processing
< 120,000	3-Quad Xeon, 2 GB RAM, 3 or more hard drives (10,000+ RPM) for email processing
< 240,000	6-Quad Xeon, 2 GB RAM, 3 or more hard drives (10,000+ RPM) for email processing

Partitioning the server

Websense Email Security frequently reads from and writes to the disk as it processes email. Therefore, a server capable of fast disk I/O is recommended. You can further optimize Websense Email Security performance by installing it on a server configured to support multiple hard drives.

The following diagram shows a server with five SCSI hard drives. Two of the hard drives are in a RAID 1 configuration and are divided into three partitions:

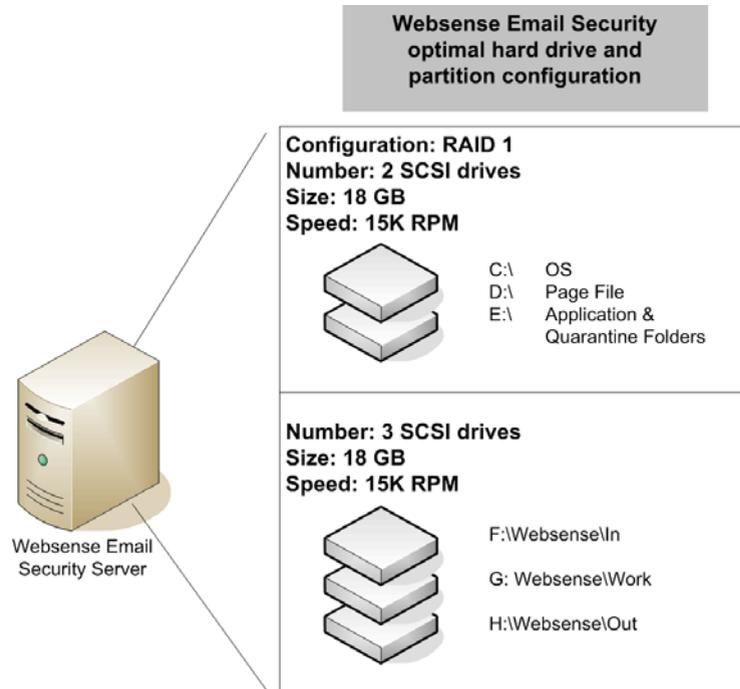
- ◆ One for the operating system
- ◆ One for the page file
- ◆ One for the Websense Email Security application

The other three hard drives each have a single partition, and are capable of fast disk I/O. The first drive contains the In folder, where Websense Email Security stores the received email messages. The second drive contains the Work folder. Websense Email

Security retrieves email messages from the In folder and moves them to the Work folder, where the messages are processed against the rule set.

Websense Email Security then moves the email to a quarantine folder for review or to the Out folder for delivery. The third drive contains the Out folder, where Websense Email Security relays processed email messages to the intended recipient.

The figure below shows the optimal hard drives and partitioning configuration for Websense Email Security.



Partitioning the Websense Email Security server

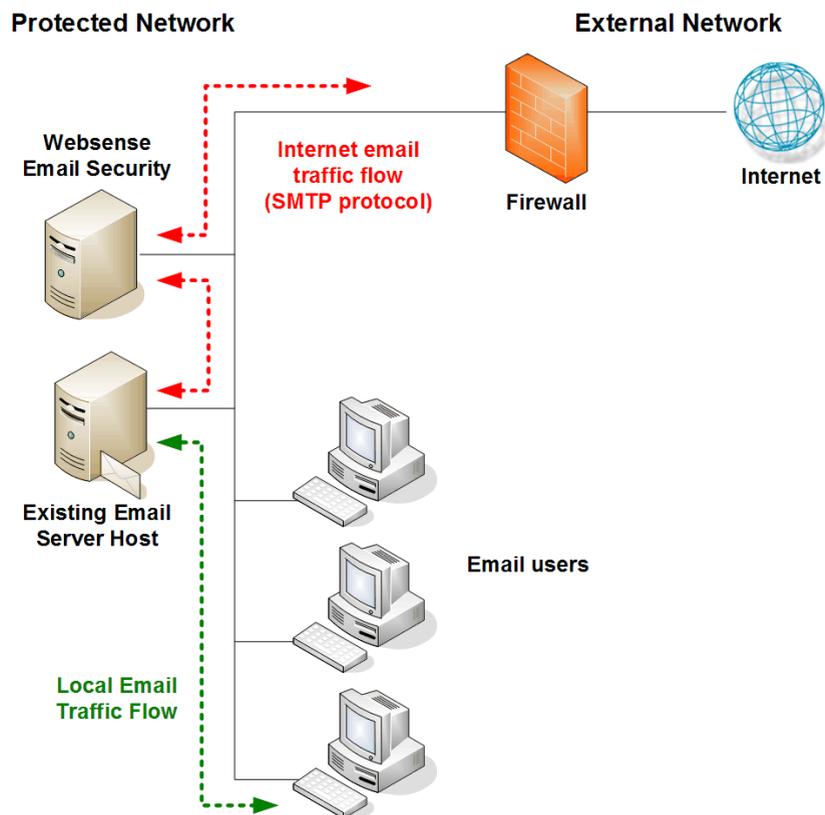
Deployment recommendations

Websense, Inc., recommends that you deploy Websense Email Security on a dedicated server. To allow the software to process email immediately, do not use this server as either an email server or a Web server. See the following sections for descriptions of deployment options:

- ◆ [Dedicated Websense Email Security deployment](#), page 19.
- ◆ [Websense Email Security deployment in a DMZ](#), page 21.
- ◆ [Multiple Websense Email Security servers](#), page 22.
- ◆ [Installing on Windows 2000](#), page 27.

Dedicated Websense Email Security deployment

In this deployment scenario, the existing email server forwards all email to Websense Email Security. Typically, changes to email clients are not needed.



Websense Email Security on a dedicated server

Run the Websense Email Security Setup Wizard and the Configuration Wizard, then configure your inbound and outbound connections, and configure the firewall to permit necessary traffic.

Inbound connections

Configure your systems for inbound traffic.

1. Direct all inbound email traffic to the Websense Email Security server.
 - If your network has an upstream SMTP gateway (not shown in the figure) between the Websense Email Security server and the firewall, configure the gateway to direct all inbound SMTP to the Websense Email Security server.
 - If your network does not have an upstream SMTP gateway, configure the firewall to direct all inbound SMTP traffic to the Websense Email Security server instead of the email server host.
2. Test this connection by sending email from an external account, such as a Webmail account.

Outbound connections

Configure your systems for outbound traffic:

1. Configure the email server host to direct outbound SMTP traffic on port 25 (or other configured port) to the Websense Email Security server. The Websense Email Security server is identified by either its server name or IP address.
2. Configure the firewall to accept outbound SMTP traffic only from the Websense Email Security server or the SMTP gateway, if a gateway is installed.
3. Test the connection by sending an email to an external account.

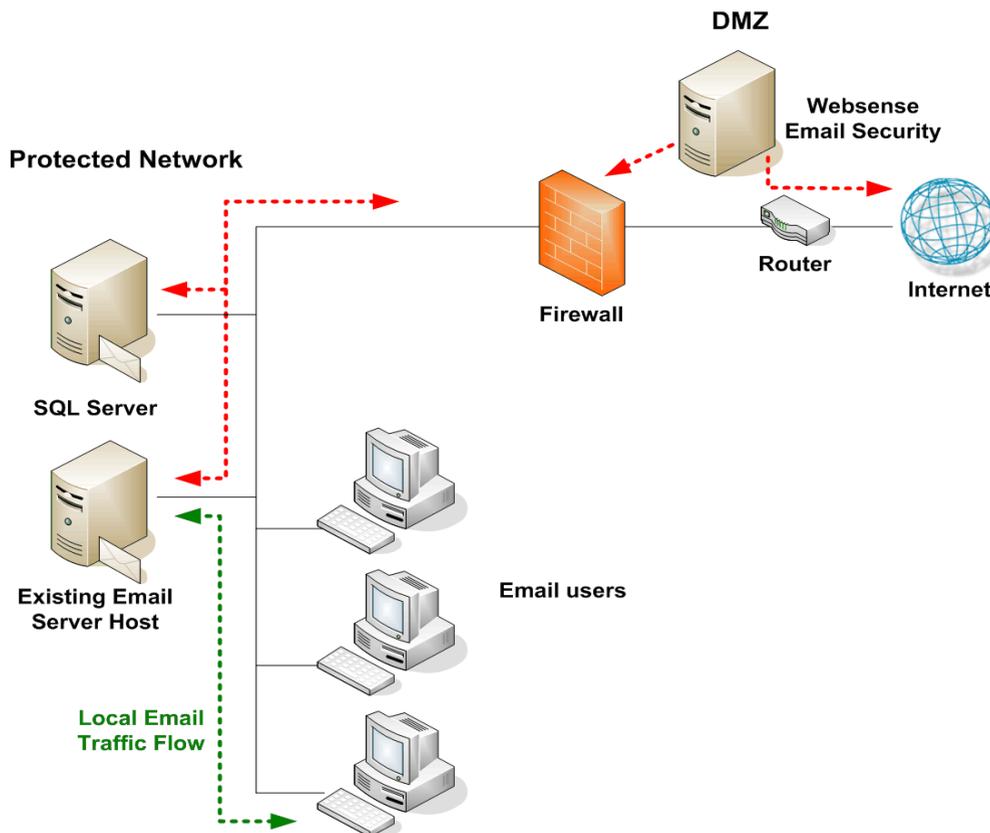
Firewall configuration

Configure your firewall to allow the following ports.

Traffic	Default Port	Protocol	Inbound	Outbound
SMTP	25	TCP	✓	✓
DNS	53 ¹	UDP		✓
HTTP	80	TCP	✓	✓

1. You do not need to allow port 53 if your network uses an internal DNS.

Websense Email Security deployment in a DMZ



Websense Email Security in a DMZ

Database connections

For Websense Email Security in the DMZ to communicate with the SQL Server, you must configure a tunnel on the firewall for the appropriate ports.

- ◆ If SQL Server is the default instance: TCP/IP port 1433 (default)
- ◆ If SQL Server is a named instance: TCP/IP port assigned to that instance, and UDP port 1434
- ◆ If SQL Server listens over named pipes: UDP ports 445 and 139

Inbound connections

The firewall has the inbound port 25 tunnel configured to the Websense Email Security server IP address (in the DMZ). A tunnel on port 25 from the Websense Email Security server to the email host is also configured.

Outbound connections

The firewall has a tunnel configured for port 25 from the email host to the Websense Email Security server in the DMZ. A tunnel for port 25 is also configured from the Websense Email Security server in the DMZ to the Internet.

Relaying email

The existing email host is configured to relay all email through Websense Email Security. Typically, changes to the email clients are not needed.

Multiple Websense Email Security servers

Some organizations install multiple Websense Email Security servers, one for each email server. These organizations can choose from two database deployment approaches.

- ◆ To provide redundancy, see [Multiple servers deployed for redundancy, page 22](#).
- ◆ To centralize databases, see [Multiple servers with centralized databases, page 25](#).

Multiple servers deployed for redundancy

This deployment eliminates the potential for a single point of failure by using both a centralized SQL Server and local SQL Server Express installations on each Websense Email Security server, as follows:

- ◆ Centralized SQL Server houses the STEMLog, STEMFriendlyName, and STEMDashboard databases.



Note

Be sure to configure failover for SQL Server to avoid loss of log data or Dashboard if that server is unavailable.

- ◆ Local SQL Server Express houses the STEMConfig database for the associated Websense Email Security server.

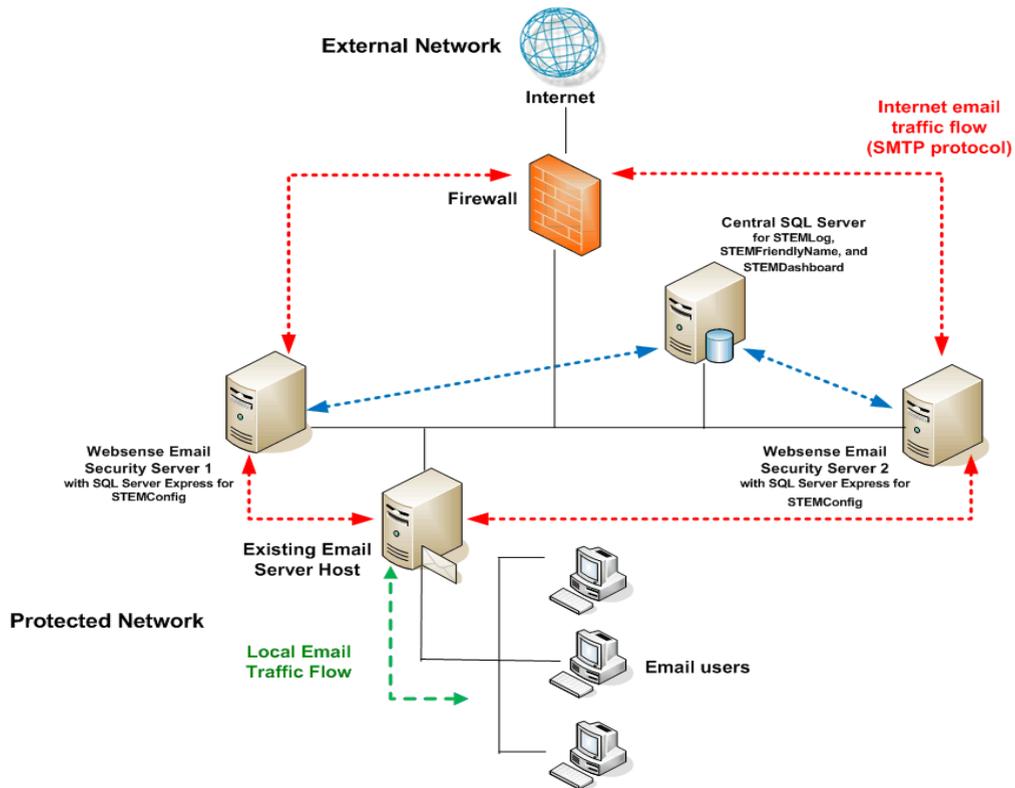


Important

Any configuration and rule changes on one of the Websense Email Security servers will **not** be automatically applied to other servers. You must make those changes separately on each server you want them to affect.

Additionally, **do not** enable the Always Allow and Always Delete end-user option in Personal Email Manager. These lists interact with only one STEMConfig database, and cannot be applied universally when multiple STEMConfig databases are used.

In this scenario, email continues to flow, even if the central SQL Server becomes unavailable.



Multiple servers deployed for redundancy

Prerequisites

The following must be true for **all** instances of Websense Email Security when deployed in this manner:

- ◆ All must have the same version, service pack level, and hotfixes.

Inbound connections

The firewall has the inbound port 25 tunnel configured to each Websense Email Security server's IP address. A tunnel on port 25 from the Websense Email Security servers to the email hosts is also configured.

In this scenario, you have 2 MX records with equal preferences set. See [Load balancing methods, page 15](#), for more information.

Outbound connections

The firewall accepts outbound SMTP connections only from the Websense Email Security servers. A tunnel for port 25 is configured from the Websense Email Security servers to the Internet.

Relaying email

The existing email hosts are configured to relay all email through Websense Email Security servers. Typically, changes to the email clients are not needed.

Scheduled tasks

The following scheduled tasks should be configured in Websense Email Security.

- ◆ On one Websense Email Security server, configure the following scheduled tasks for the STEMLog database:
 - Database maintenance tasks such as Purge, Archive, and Shrink
 - Index maintenance
- ◆ On every Websense Email Security server, configure a scheduled task to download the database for each of the following features that is subscribed:
 - Anti-Spam Agent (every 30 minutes)
 - Anti-Virus Malware Scanning (every 30 minutes)
 - Master Internet Threat Database update (once per day)
 - Real-time Internet Threat Database (every 30 minutes)
 - Anti-Virus Agent (every 30 minutes)
- ◆ On every Websense Email Security server, configure a scheduled task for Queue Synchronization (once per week).

There should be no time overlap for the Queue Synchronization tasks.

Service configuration

Each of the Websense Email Security services must be configured to log on as an account with the following permissions:

- ◆ administrative rights to the local machine
- ◆ database owner (DBO) rights to the databases

For each service, open the Windows Services dialog box, and select Properties to set its Log On account.

Additional considerations

Only one Websense Email Security administrator can access any given quarantined message. Once the message is loaded into an instance of the Message Administrator or the Web Administrator, it is locked for all other administrators.

This configuration is scalable to use more than 2 Websense Email Security servers.

Multiple servers with centralized databases

This deployment simplifies system maintenance by using a centralized SQL Server to house all Websense Email Security databases: STEMConfig, STEMLog, STEMFriendlyNames, and STEMDashboard.

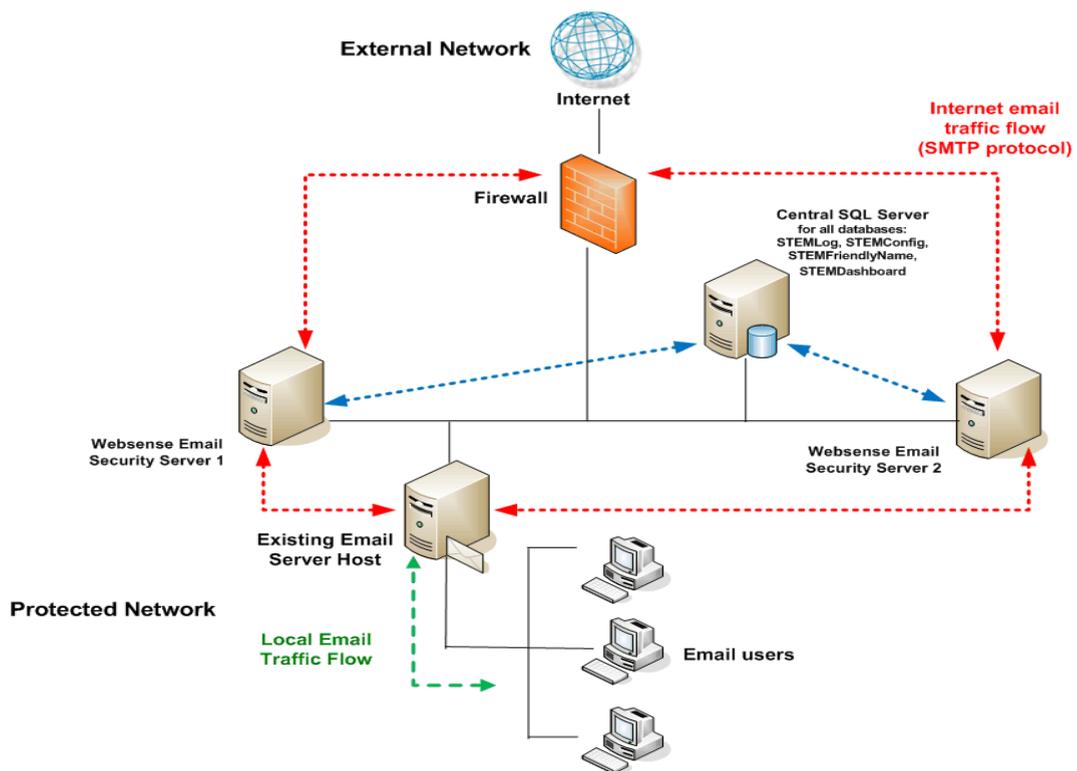
By using a centralized STEMConfig database, you can make server configuration or rule changes on any instance of Websense Email Security server to update all servers simultaneously.



Important

If the SQL Server becomes unavailable in this deployment, email **stops** flowing.

All Personal Email Manager features are supported when the databases are all centralized.



Multiple servers with centralized databases

Prerequisites

The following must be true for **all** instances of Websense Email Security when deployed in this manner:

- ◆ All must have the same version, service pack level, and applied hotfixes.
- ◆ All must use the same installation drive, installation path, and queue paths.

Inbound connections

The firewall has the inbound port 25 tunnel configured to each Websense Email Security server's IP address. A tunnel on port 25 from the Websense Email Security servers to the email hosts is also configured.

In this scenario, you have 2 MX records with equal preferences set. See [Load balancing methods, page 15](#), for more information.

Outbound connections

The firewall accepts outbound SMTP connections only from the Websense Email Security servers. A tunnel for port 25 is configured from the Websense Email Security servers to the Internet.

Relaying email

The existing email hosts are configured to relay all email through Websense Email Security servers. Typically, changes to the email clients are not needed.

Scheduled tasks

The following scheduled tasks should be configured in Websense Email Security.

- ◆ On one Websense Email Security server, configure the following scheduled tasks for the STEMLog database:
 - Database maintenance tasks such as Purge, Archive, and Shrink
 - Index Maintenance
- ◆ On every Websense Email Security server, configure a scheduled task to download the database for each of the following features that is subscribed:
 - Anti-Spam Agent (every 30 minutes)
 - Anti-Virus Malware Scanning (every 30 minutes)
 - Master Internet Threat Database update (once per day)
 - Real-time Internet Threat Database (every 30 minutes)
 - Anti-Virus Agent (every 30 minutes)
- ◆ On every Websense Email Security server, configure a scheduled task for Queue Synchronization (once per week).

There should be no time overlap for the Queue Synchronization tasks.

Service configuration

Each of the Websense Email Security services must be configured to log on as an account with the following permissions:

- ◆ administrative rights to the local machine
- ◆ database owner (DBO) rights to the databases

In the Windows Services dialog box, right-click each service and select Properties to set its Log On account.

Additional considerations

Only one Websense Email Security administrator can access any given quarantined message. Once the message is loaded into an instance of the Message Administrator or Web Administrator, it is locked to all other administrators.

This configuration is scalable to use more than 2 Websense Email Security servers.

Installing on Windows 2000

When installing Websense Email Security on a Windows 2000 server, you need to disable and stop the SMTP service in the following circumstance:

You can install Websense Email Security to communicate over any port, but you must first stop and disable any other service using that port.

For example, the SMTP service uses port 25, which is the same port that Websense Email Security uses by default. Disable and stop the SMTP service before you install Websense Email Security to use port 25; otherwise, Websense Email Security cannot start.

To disable and stop the SMTP service on a Windows 2000 server:

1. In the Windows control panel, choose **Administrative Tools > Services**.
2. On the list of services, double-click **Simple Mail Transport Protocol (SMTP)**. The properties dialog box appears.
3. Open the **General** tab.
4. From the **Startup type** drop-down list, select **Disabled**.
5. Click **Stop**.
6. Click **OK**.

Preparing to import users and groups (optional)

After installation is complete, your site can set up customized filtering rules. That process is simplified if you have prepared an optional database of your users and groups. You can import this database into the Rules Administrator during rule setup.

Use the following procedure to create the database of users and groups after you install Websense Email Security.

1. Run the batch file **ScoutGroupDB.bat** to create the ScoutGroupDB database, which contains a single table, named EmailAddress.

The default path is:

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

2. Create System Data Source Name (DSN) **ScoutGroup** on the same computer as Websense Email Security:
 - a. In the Windows Control panel, select **Administrative Tools > Data Sources (ODBC)**.

- b. Select the **System DSN** tab, and then click **Add**.
- c. Select **SQL Server** from the list, and then click **Finish**.
- d. Enter the details of the data source, and then click **Next**.
- e. Use the same logon authentication details set during Websense Email Security server installation, and then click **Next**.

If you have not yet installed Websense Email Security server, remember the logon authentication details you enter here to use during that installation.

- f. Follow the onscreen instructions to complete the Wizard.
- g. Ensure that the configuration in the final screen is correct, and then click **OK**.

The Rules objects use the same authentication details as the Websense Email Security setup.

3. Open the database management console for your version of SQL Server, and fill out the following EmailAddress table fields for each user:
 - **[Email]** – Enter the email address of the user. For example, bill@company1.com.
 - **[EmURules]** – Enter the group names for the user. This is semicolon delimited. For example, Sales;Marketing;Admin.

Implementing rules using these users and groups

To use these users and groups in the Websense Email Security rules, follow the instructions in the *Websense Administrator Help*. Go to **Rules Objects > Who objects > Retrieving user information from a data source**.

2

Installation

Use the information in this chapter to upgrade, install, or rollback to your previous version of Websense Email Security.

Installation options

Install all components (server and administrative client), or only the client:

- ◆ Websense Email Security Server – A complete installation of all components; see [Installing Websense Email Security, page 31](#).
- ◆ Administration Client only – For remote monitoring and administration of the Websense Email Security server; see [Installing the Administration Client, page 39](#).

The Administration Client is automatically installed when you install the Websense Email Security Server. You can install additional instances of the Administration Client on different machines by selecting a Client-only installation.

Configuration after installation

After a new installation, the Configuration Wizard runs automatically, enabling you to set parameters for Websense Email Security. See [Websense Email Security Configuration Wizard, page 35](#), for guidelines on completing this wizard. If you need additional information, see the [Configuration Wizard Help](#).

Upgrading from an earlier version of Websense Email Security preserves the parameters from the previous installation. The Configuration Wizard does not run after an upgrade.

If configuration changes are needed later, run the Monitor and select the Server Configuration icon. See [Websense Email Security Administrator Help](#) for additional information.

Upgrading from earlier versions

You can upgrade to Websense Email Security directly from Websense Email Security version 7.0 or 7.1.

If you are upgrading from Websense Email Security v7.0 or v7.1, be sure to upgrade Personal Email Manager and Report Central after the Websense Email Security upgrade. Installers and installation instructions for these modules are provided with the Websense Email Security version 7.2 product. The installers for Report Central and Personal Email Manager are located in the folder to which the installation files are extracted (typically, C:\Websense).

If you are running Websense Email Security version 6.1 or an earlier SurfControl E-Mail Filter version, you must upgrade first to Websense Email Security version 7.0 or 7.1, and then to Websense Email Security version 7.2. Go to the Support Portal at www.websense.com for detailed instructions on interim upgrades.

If this is a new installation, go to *Installing Websense Email Security*, page 31.

Upgrading the server

To upgrade the Websense Email Security server:

1. Download the Websense Email Security installation package from www.MyWebsense.com.
2. After you extract the installation files, **setup.exe** starts the Websense Email Security Setup Wizard automatically.

The new files are installed to the same folder as the previous version.

3. Select **Upgrade to Websense Email Security v7.2**, and then click **Next**.
4. Enter the **Windows User Account** information to identify an account that has administrator privileges on the installation machine or domain, and then click **Next**.

Ideally, this should be the same user name, password, and domain or machine name configured during initial setup for running other Websense Email Security services. To find that account name, open the Windows Services dialog box and double-click a Websense Email Security service name. In the Properties dialog box, click the Log On tab to find the account name.

5. Choose whether to enable **SystemSynch**, and then click **Next**.

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

SystemSynch never sends information that would identify specific users.

6. Click **Yes** to confirm the upgrade.
 - Services from the previous version are stopped, and the existing databases and files are backed up. This may take a few minutes.

Do not delete or move these backup files, because they are necessary in the event that you desire to roll back to your previous version. See [Rolling back to your previous version, page 41](#).
 - The Setup Status screen shows the progress of the setup.
 - Websense Email Security downloads the latest content for specific Websense Email Security functions.
7. Click **Next** after the downloads are complete.
8. After the upgrade finishes, click **Next**.
9. Click **Finish** in the Upgrade Complete screen.

Remember to upgrade your Personal Email Manager and Report Central installations.

Upgrading the client

To upgrade the Administration Client:

1. Uninstall the current Administration Client via the Add or Remove Programs option in the Windows Control Panel. Uninstall any hotfixes first, then the main program.
2. Run the Websense Email Security version 7.2 installer, and choose the **Client only** setup type. See [Installing the Administration Client, page 39](#).

Possible upgrade interruption

If your system does not meet the minimum or recommended specifications, one of the following messages is displayed. Please see [System requirements, page 9](#).

- ◆ **ERROR** – An error appears if a required component is missing. This message is typically triggered by an incorrect operating system or service pack level. You must exit the installer and correct the problem before running the installer again, or run the installer on a machine that meets the requirements.
- ◆ **WARNING** – A warning appears if you have the minimum, but not the recommended, memory or disk space. The installation is not stopped.
- ◆ **INSTALL** – An install message appears if a component, such as an MDAC component, has not been detected and will be installed with Websense Email Security. You may be instructed to restart after the installation.

Installing Websense Email Security

For a new installation of all Websense Email Security components, complete the following wizards:

- ◆ Websense Email Security Setup (see *Websense Email Security Setup Wizard*, page 32)
- ◆ Websense Email Security Configuration (see *Websense Email Security Configuration Wizard*, page 35)

If you are upgrading from a previous version of Websense Email Security, go to *Upgrading from earlier versions*, page 30.

Websense Email Security Setup Wizard

Websense Email Security requires a Microsoft SQL Server system to store rules, system configuration, and dictionaries. You can use an existing SQL Server installation, or you can install Microsoft SQL Server 2005 Express SP2 from the Websense Email Security Setup wizard.



Note

If you choose to connect to an existing installation of SQL Server 2000 SP4, SQL Server 2005 SP2 or SP3, or SQL Server 2008 SP2 on a different machine, database tools will be installed on the local machine, if they are not already present.

To install SQL Server 2005 Express SP2 on the local machine, Microsoft Windows Installer 3.1 and Microsoft .NET Framework 2.0 or later must already be installed (see the Microsoft Web site for information).

1. Download the Websense Email Security installation package and obtain a subscription key from www.MyWebsense.com.
2. Double-click the installation package to extract the files.
3. Accept the default folder for the installation files, or choose a different folder. Then, click **Next**.
The Setup Wizard launches automatically.
4. In the Setup Welcome screen, click one of the buttons to open the relevant document in a separate window, if desired. Then, click **Next**.
 - **Readme** – Details of enhancements and technical improvements for this release.
 - **Getting Started Guide** – An online copy of this Installation Guide.
5. Accept the terms of the Websense Subscription Agreement, and then click **Next**.
6. Choose whether to enable SystemSynch, and then click **Next**.

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

SystemSynch never sends information that would identify specific users.

7. Choose an installation type and location, and click **Next**.
 - **Server and client** – Installs the Websense Email Security server and all Administration Client applications. Continue with the next step.
 - **Client only** – Installs only the selected Administration Client components. For example, you might install only the Rules Administrator component on a separate machine, so that you can set up rules remotely. Go to [Step 5, page 39](#), under *Installing the Administration Client*.
 - **Destination Folder** – Accept the default path (C:\Program Files\Websense Email Security\), or click **Browse** to select a different path.

8. Your system is checked against the requirements. See *System requirements*, page 9.

If your system does not meet the minimum or recommended specifications, one of the following messages is displayed.

- **ERROR** – An error appears if a required component is missing. This message is typically triggered by an incorrect operating system or service pack level. Click **Cancel** to exit the installer. Correct the problem and run the installer again, or run the installer on a machine that meets the requirements.
- **WARNING** – A warning appears if you have the minimum, but not the recommended, memory or disk space. The installation is not stopped. Click **Next** to proceed.
- **INSTALL** – An install message appears if a component, such as an MDAC component, has not been detected and will be installed with Websense Email Security. You may be instructed to restart after the installation. Click **Next** to proceed.

If your system passes the system check, no message is displayed. Click **Next** to proceed.

9. In the Configure Database screen, choose one of the options presented, and proceed as indicated below.
 - If no compatible version of Microsoft SQL Server is detected on the local computer, an option is provided to install SQL Server 2005 Express SP2. See [Step 10](#).
 - If a supported version of SQL Server is found on the machine, an option is provided to create the Websense Email Security databases locally. See [Step 11](#).
 - An option is also provided to create the Websense Email Security databases on another machine running a supported version of SQL Server. See [Step 12](#).
10. Click **Next** to launch the SQL Server 2005 Express SP2 installation.
 - a. Click **Yes** to continue.

If you click **No**, the Setup Wizard returns to the Websense Email Security installation and prompts you to connect to an existing database installation.
 - b. Select a location to install SQL Server 2005 Express SP2, and then click **Next**.

- c. Enter a database password for the system administrator (SA) account, and then click **Next**.

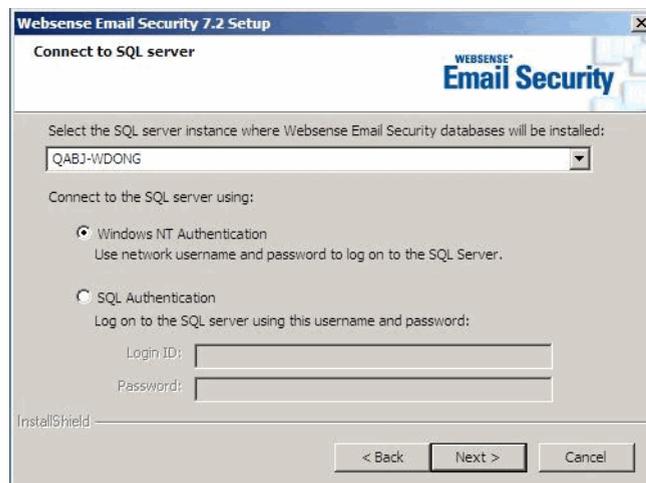
You should note that Windows Server 2008 has more complex password requirements from earlier versions. If you are using SQL Server 2005 with Windows Server 2008, you must enter a password that meets the complexity requirements. See [SQL Server or SQL Server 2005 Express, page 14](#) for information about complex passwords for Windows Server 2008.

- d. Enter the logon information for a network account that has administrative access to the machine, and then click **Next** to start the installation.

Progress screens are displayed as the installation runs.

- e. Go to [Step 13](#).

11. Click **Next** to display the Connect to SQL Server screen. Go to [Step 12b](#) to complete the database connection.
12. Click **Next** to use an instance of SQL Server elsewhere in the network. The Setup Wizard searches the network for SQL Server running on other machines. When the servers are located, the Connect to SQL Server screen requests connection information.



- a. Select a SQL Server instance from the drop-down list.
- b. Select a connection method for SQL Server, either Windows or SQL authentication.
- If you select **SQL Authentication**, ensure that SQL Server is running in mixed mode.
 - Enter the **Login ID** and **Password**.

The login ID must represent an account that is DBO and has system administrator permissions in SQL Server, such as the SA account.

- c. Click **Next**.

13. Click **Next** in the summary screen to begin installing the Websense Email Security files. A progress bar shows the status of the installation.
14. In the Installation Complete screen, clear the **View README** check box if you do not want to open the README file. Then, click **Finish**.

You may be prompted to restart the computer.

The Websense Email Security Configuration Wizard opens. See the next section, [Websense Email Security Configuration Wizard](#).

Websense Email Security Configuration Wizard

Use the Configuration Wizard to set the parameters for Websense Email Security and prepare your site for email filtering.

The Configuration Wizard requests information in four sections:

- ◆ Your Organization
- ◆ System Details
- ◆ Mail Routing
- ◆ Filtering Options

From any Configuration Wizard screen, you can:

-  ◆ Click the help button for information about the fields and tasks in each screen.
- ◆ Click **Cancel** to stop the wizard. The settings that you have entered to that point are saved.

The Configuration Wizard is launched automatically after Websense Email Security Setup installation. It can also be launched separately.

1. If it is not already running, start the Configuration Wizard: **Start > Programs > Websense Email Security > Configuration Wizard**.
2. Open the configuration checklist in the Welcome screen. Gather the requested information for use in later Configuration Wizard screens.
3. Click **Next**.
4. In the Subscription Key screen, enter the Websense subscription key provided when you downloaded the software. Then, click **Next**.

This subscription key enables the base product and all optional ThreatSeeker components in your subscription.

Go to www.MyWebsense.com if you have lost the key.

5. In the Administrator Account screen, create a Websense Email Security account that will have full permissions to the Dashboard and all client applications. Then, click **Next**.
 - **User name** – Enter the user name for the new account.
 - **Password** – Enter a password for this account.
 - **Confirm password** – Enter the password again, with the same spelling and capitalization.
 - **Email address** – Enter the address that can be used for sending alerts from the Dashboard.
6. Click **Next** in the System Details screen.

7. In the Windows User Account screen, enter the information listed below. Then, click **Next**.
 - **User name** – Enter the user name for a Windows account with administrative privileges to start Websense Email Security services.
 - **Password** – Enter the password for this account.
 - **Domain or machine name** – Enter either the domain name or the computer name of the machine where Websense Email Security is installed. The name of the local computer appears automatically.

You must enter valid information to move to the next screen.

8. Accept the default Administration Service Port (8181), or enter an alternate port number, and then click **Next**.

Websense Email Security uses a Web services port to manage its internal communications and control Remote Administration.

You must enter an available port to move to the next screen.

9. Click **Next** in the Mail Routing screen.

10. In the SMTP Port screen, select a port number option, and then click **Next**.

Websense Email Security uses this port to listen for incoming email.

Select either:

- **Use Port 25** – After you select this option, the wizard verifies whether the port is available.
- **Use a different port** – Select this option, and then enter a different port if port 25 is in use. The wizard verifies whether the port is available.

You must select an available port to move to the next screen.

11. In the Protected Domain screen, enter the following details about the main email domain that you want Websense Email Security to protect.

- a. Enter the domain information:

- **Email domain** – Name of the domain you want to protect from email threats. For example: mycompany.com
- **Postmaster email address** – Email address for the administrator of the local domain. For example: postmaster@mycompany.com
- **Name or IP address of mail server** – Name or IP address of the email server for your domain. For example: mail.mycompany.com
- **Mail server SMTP port** – The SMTP port that Websense Email Security should use to communicate with the email server. The default is 25.

- b. Click **Test** to check the connection.

If the test fails, verify that the domain information has been entered correctly, then, run the test again.

If the information is correct and the test still fails, try testing connectivity to the mail server via a telnet test on the port specified in the previous step. After correcting any connectivity problems, test the connection again through the Configuration Wizard.

- c. Click **Next** after the test is successful.

See the *Websense Email Security Administrator Help* for instructions on adding more email domains to the Protected Domain list.

12. In the Outbound Mail Delivery screen, select how Websense Email Security sends outbound email messages to the Internet. Then, click **Next**.

- a. Choose an option:

- Send outbound email directly to the Internet. Perform a DNS lookup to resolve the email address.
- Send outbound email to another email server (mail relay). That email server handles domain name resolution and any further routing.

To route outbound mail through another email server, specify:

Host Name or IP – The host name or IP address of the email server to which you want email forwarded

Port – The port that Websense Email Security should use to communicate with that email server

- b. Click **Test** to check the connection.

- c. Click **Next** after the test is successful.

See the *Configuration Wizard Help* for instructions on adding more mail relay hosts.

13. Click **Next** in the Filtering Options screen.

14. In the Activate Rules screen, select the standard rules to enable immediately. Then, click **Next**.

Websense Email Security is installed with a set of standard rules. Using these rules, you can protect your system from common threats as soon as the product is running.

- **Enable Spam Filtering Rules** – Block spam and phishing emails.
- **Enable Virus Protection Rules** – Block email messages that carry known viruses and malware.
- **Enable Network Security Rules** – Prevent looping, unauthorized encryption, and other security threats.

See the *Websense Email Security Administrator Help* for instructions on fine-tuning the rules to meet the requirements of your Acceptable Use Policy.

15. In the Queue Folder for Isolated Email screen, accept the default folder location, or click **Browse** to choose a different location. Then, click **Next**.

If an email triggers a rule, the message can be held in a queue folder, where you can inspect it and take action.

The Configuration Wizard checks the computer for disk space, and suggests a path on the drive where the most disk space is available, if appropriate.

16. In the Automatic Queue Management screen, select options for deleting email messages automatically from the Spam or Virus queues. Then, click **Next**.

- **Delete messages in the Virus queue after 7 days**
- **Delete messages in the Spam queues after 14 days**

See the *Websense Email Security Administrator Help* for instructions on queue management.

17. In the Automatic Database Management screen, select whether to automatically purge the log database. Then, click **Next**.

Marking the **Purge Database Weekly - Purge data older than 30 days** check box helps optimize performance by preventing the database from becoming too large.

When Websense Email Security is running, you can change the frequency of database purges in the Scheduler. See the *Websense Email Security Administrator Help* for details on Scheduler functions.

18. Enter an email address for Websense Email Security to notify an administrator when a system event occurs. Then, click **Next**.

These events are:

- Message buildup in queue folders
- Scheduled event status

19. In the Ready to Configure screen, click **Start** to implement the options selected in the Configuration Wizard.

This process may take a few minutes.

**Note**

If you do not want to implement the configuration settings immediately, click **Cancel**. The Configuration Wizard saves your settings so that you can run the wizard another time to implement the settings.

If an event fails:

- Click **Back**, and amend the relevant details.
- Click **Retry** to retry the configuration without amending any details.
- Click **Skip** to omit the configuration of the current event and continue to the next event.

20. After the configuration is complete, click **Next** to display the Real Time Anti-Virus Scanning screen.

Ensure that Websense Email Security working directories (in, out, work, and temp) have been excluded from real-time anti-virus scanning.

To verify that the correct folders have been excluded, click **Check Folders**.

Websense Email Security tests the work folder, which is 1 of the 4 folders that need to be excluded from Real Time Anti-Virus Scanning. Then, follow the onscreen instructions.

- If a folder is correctly excluded from real time anti-virus scanning, you see the message **Test OK**.
- If the folder is being scanned by anti-virus software, an error message is displayed.

Exclude this folder from anti-virus scanning as directed by the anti-virus documentation; otherwise Websense Email Security cannot handle virus-infected files and malware correctly.

21. Click **Next**.
22. Click **Finish** in the Configuration Complete screen.

After running the Configuration Wizard, you can use the Websense Email Security Monitor to make any configuration changes.

Installing the Administration Client

To install selected Websense Email Security components for remote administration:

1. If you have not already downloaded the Websense Email Security installation package, see [Websense Email Security Setup Wizard, page 32](#), steps 1 – 3, for a description of this process.

The Setup Wizard launches automatically.

2. Click **Next** in the Welcome screen.
3. Accept the terms of the subscription agreement, and then click **Next**.
4. Choose **No** when asked to enable SystemSynch, and then click **Next**.
SystemSynch operates only on the Websense Email Security server, so is not needed on a machine running only the Administration Client.
5. Select **Client only** in the Setup Type screen, and select the **Destination Folder**. Then, click **Next**.

By default, the components are installed in the following folder

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

For the x64 platform, the default installation folder is

```
C:\Program Files(X86)\Websense Email Security
```

6. In the Components screen, clear the check box for any components that are not needed, and then click **Next**.

All Administration Client components are selected by default. You can install all of the components or just selected components. For example, you can select to install only the Rules Administrator component to enable a user to set up rules remotely.



7. Your system is checked against the requirements. See [System requirements](#), page 9.

If your system does not meet the minimum or recommended specifications, one of the following messages is displayed.

- **ERROR** – An error appears if a required component is missing. This message is typically triggered by an incorrect operating system or service pack level. Click **Cancel** to exit the installer. Correct the problem and run the installer again, or run the installer on a machine that meets the requirements.
- **WARNING** – A warning appears if you have the minimum, but not the recommended, memory or disk space. The installation is not stopped. Click **Next** to proceed.
- **INSTALL** – An install message appears if a component, such as an MDAC component, has not been detected and will be installed with Websense Email Security. You may be instructed to restart after the installation. Click **Next** to proceed.

If your system passes the system check, no message is displayed. Click **Next** to proceed.

8. Enter the details of your Websense Email Security server in the Configure Remote Access screen:

- **Server name or IP address**
- **Port number**
- **User name**
- **Password and Confirm Password**

These details enable users on this computer to log on to the Websense Email Security server and use the selected Websense Email Security administration components.

9. Click **Next** in the summary screen to begin installing the Websense Email Security files.

If you need to change any details, click **Back**.

10. In the Installation Complete screen, clear the **View README** check box if you do not want to open the README file. Then, click **Finish**.

You may be prompted to restart the computer after the installation.

Rolling back to your previous version

You can roll back to your previous version of SurfControl E-mail Filter (version 6.0 SP1 or earlier) or Websense Email Security (version 6.1 SP1 or later).

If you would like to back out of an upgrade, use the Windows Add/Remove Programs function.

1. In the Windows Control Panel, select **Administrative Tools > Add/Remove Programs**.
2. Select **Websense Email Security**.
3. Select the Rollback option to return to the previous version.

If you upgraded to Websense Email Security v7.2 from Websense Email Security version v7.0 or v7.1, the upgrade process backed up STEMConfig and other necessary files.

After the upgrade, you may have changed the product's configuration, and some messages may have been received and isolated. In the rollback process, Websense Email Security reverts back to the previously installed version. Backup copies of files, including STEMConfig, are restored. The Log Database (STEMLog) contains all messages that have been isolated since the upgrade. No email messages are lost.



Note

A restart is needed after rollback, if the files that need to be rolled back to a previous version are locked by other processes.
