Release Notes for Websense Email Security v7.2

Websense Email Security version 7.2 is a feature release that includes support for Windows Server 2008 as well as support for Microsoft SQL Server 2008. Version 7.2 also contains other enhancements, along with several stabilizing fixes. This Release Notes document describes enhancements and fixed issues, along with some tips for upgrading from prior versions of Websense Email Security.

Websense Email Security includes the Personal Email Manager tool for end-user management of quarantined messages and the Report Central reporting package. Personal Email Manager is released as version 7.2. Report Central version 2.7.2 is released with Websense Email Security version 7.2. Both components include some new features and fixes, including support for Windows 2008. See *Personal Email Manager and Report Central* in these Release Notes for information about changes to these tools.

Topics covered in this paper include the following:

Key features in this release

Tips for upgrading from prior versions

Supported software

Fixed issues

Release Notes additions

Click here for a list of known issues in Websense Email Security v7.2 is available. You will be prompted for your MyWebsense credentials.

Key features in this release

Websense Email Security version 7.2 includes such functional enhancements as support for Windows Server 2008 and Microsoft SQL Server 2008. This release also contains the new features described in this section. For information on all Websense Email Security features, see the Websense Email Security Help menu, or the Websense Email Security Administrator Help.

Windows Server 2008 and SQL Server 2008 support

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. You must enable standard file sharing and network discovery for Websense Email Security to function properly in a cluster configuration running Windows Server 2008.

You can enable file sharing and network discovery in the Windows Network and Sharing Center 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. See “SQL Server behind a firewall,” in the Websense Email Security *Installation Guide* for more information.

Encryption gateway rule

A new predefined encryption gateway rule can redirect email to a specified Smart Host server for encryption. When Websense Email Security detects an email message that meets the criteria you specify for encryption, this rule is triggered. The encryption server encrypts the redirected email and sends it to its destination.

Message search only option in Message Administrator

You can now set up Websense Email Security user accounts that include permission to release messages via a message search in the Message Administrator without the permission to view message content. A new Message Search Only option is included in the Message Search function of Message Administrator.

Zero-Hour Protection function renamed

The Zero-Hour Protection component of the Anti-Virus Malware Scanning rule object is renamed to Websense Internet Threat Database Real-Time Protection. This component continues to protect your system from emerging outbreaks of email-borne viruses contained in URL links. It determines potential threats based on real-time URL categorization.

Proxy information edit

You can change the proxy server user name and password that you entered in the Configuration Wizard at product installation. Select the Monitor **Tools > Options** to edit the user name and password.

Personal Email Manager and Report Central

Websense Email Security version 7.2 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.

Personal Email Manager

Personal Email Manager version 7.2 is now supported on Windows Server 2008. This end-user component also allows users to specify a SQL Server instance name during product installation. The instance name can be entered along with the port information in the SQL Server Connection Details dialog box.

It is possible to change Personal Email Manager and Websense Email Security database server information after product installation via the Personal Email Manager Configuration Tool.

To change server database information:

Open the Personal Email Manager Configuration Tool (**Start > Programs** [or **All Programs**] **> Personal Email Manager > Configuration Tool)**.

1. Click the **PEM Database** button or the **WES Database** button, depending on which database configuration you want to modify.

2. In the resulting dialog box, edit any database server information that you want to change, including
   - the name or IP address of the database server
   - the server’s TCP port number
   - the method of authentication. If SQL authentication is used, enter the server login details.

Test your connection by clicking the **Test** button in the dialog box.

Report Central

This version of Report Central is now supported on Windows Server 2008. This component also includes a new predefined standard report. The Top N Viruses report is a traffic-based management report that can be displayed either as a horizontal bar chart or a table. This report provides the name and frequency of each virus detected based on defined date and time criteria.

Tips for upgrading from prior versions

Complete upgrade instructions are included in the Websense Email Security *Installation Guide*.

Direct upgrade is supported for the following products:

- Websense Email Security version 7.0 (with any hotfixes applied)
- Websense Email Security version 7.1 (with any hotfixes applied)

Users of Websense Email Security version 6.1 and earlier must first upgrade to Websense Email Security version 7.0 before installing version 7.2.

Client upgrades are not supported. Please uninstall the existing version of the client application and install the latest version. A subscription key is not required for client installation.

Subscription keys

The multiple-key subscription model used for Websense Email Security version 6.1 Service Pack 1 and earlier was replaced with a single-key subscription model in version 7.0. Your subscription key enables email filtering and several ThreatSeeker technologies, including:

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

Optionally, you can extend your subscription to include:

- Anti-Virus Agent
- Virtual Image Agent

If you are upgrading from version 6.1 or earlier, you must have a new subscription key before initiating the upgrade process. During the upgrade, you will be prompted for the new key. To order a new key, log on to MyWebsense.

Existing SurfControl keys will continue to function for 60 days after you obtain the new Websense subscription key.

If you are upgrading from version 7.0 or later, you are not prompted for a new key.

STEMLog database rebuild

If you are upgrading from version 7.0 or earlier, the installation process includes a step to rebuild your STEMLog database. The rebuild process can result in improved performance of database management activities, as well as Message Administrator search message and query functions. Please note that a significant amount of downtime is required for the rebuild process. For example, rebuilding a 24-GB database may take 2 hours or more.

We strongly recommend that you back up your current STEMLog database before you install version 7.2.

If you have already rebuilt the STEMLog database in conjunction with upgrades to Websense Email Security version 7.0 or version 6.1, Service Pack 1, Hotfix 6, the installation process detects that your database has been modified and does not run the rebuild process again.

Duplicate alerts

The Dashboard alert system monitors and responds to more than 30 vital system conditions, including the accumulation of messages in the drop-off and pick-up folders. Separate monitoring and reporting are still supported via Receive Service, Rules Service, and Send Service configuration. If you plan to use the Dashboard alert system, you may want to turn off these redundant alerts. In the Server Configuration console, review the **Enable Administrator alerts** settings for:

- Receive Service general setting - monitors the received mail drop-off folder (**In** folder)
- Rules Service general settings - monitors the processed mail drop-off folder (**Out** folder)
- Send Service general settings - monitors the mail pick-up folder (**Out** folder)

Internet Threat Database update tasks

As of version 7.0, the ThreatSeeker Internet Threat Database replaced the threat database from earlier versions of Websense Email Security. As part of the upgrade process from version 6.1 or earlier, the installer deletes existing “Internet Threat Database Update” Scheduler tasks, and creates two new tasks:

- Master Internet Threat Database update: runs daily at 00:30
- Real-time Internet Threat Database update: runs every 30 minutes, every day

If you are upgrading from version 6.1 or earlier, you may need to modify some scheduled tasks. To change the default schedule or create or delete a task, open the Scheduler.

To change the settings of an existing task, double-click on the task, make the desired changes, and click OK. For more information, see “Scheduling Internet Threat Database updates” in *Administrator Help*.

New Authentium Anti-Virus configuration options

In version 7.1, the Authentium Anti-Virus engine in the Anti-Virus Malware Scanning object was upgraded to the version 5.1.3 Authentium engine. As a result, the Authentium (Command Antivirus) configuration options may have changed. If you are upgrading from version 6.1 or earlier and after the upgrade process is complete, you should open any rules that use Authentium (by default: “Anti-Virus Malware Scanning - Isolate messages that contain a Virus or Malware”), open the AVMS object in the rule, select **Authentium** from the **Virus scanners** list, click **Configure,** and select the desired options. See “Configuring the Anti-Virus Malware Scanning object” in *Administrator Help*.

Anti-Virus scanning

For superior discovery of email-borne viruses, it is highly recommended that you use the default Anti-Virus Malware Scanning (AVMS) rule. AVMS uses two highly regarded third-party virus scanners, McAfee and Authentium.

If your organization requires use of another third-party scanner, please see the list of supported scanners below. For configuration information, see “Third-Party Virus Scanning object” in *Administrator Help*.

Virus Scanner Manufacturer	Scan Engine Version	Product Version
McAfee Command Line Scanner	5.2	5.2
McAfee VirusScan Enterprise	4400	8.0.0

Virus Scanner Manufacturer	Scan Engine Version	Product Version
Sophos Savi DLL*	2.52.1	7.0.5
Symantec Anti-Virus Scan Engine (SASE)	5.1	5.1.6.31

*Known issue: Versions after 7.0.5 may not be compatible with Websense Email Security version 7.0 and later.

Supported software

Servers and clients:

- Windows 2000 Server SP4
- Windows Advanced Server 2000 Service Pack 4
- Windows Server 2003 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2003 x64 Edition SP2
- Windows Server 2003 R2 x64 Edition SP2
- Windows Server 2008 SP2
- Windows Server 2008 x64 SP2

Clients only:

- Windows XP Professional SP2
- Windows 2000 Professional SP4
- Windows Vista SP1

Database servers:

- Microsoft SQL Server 2000 SP4
- Microsoft SQL Server 2005 SP2, including Express Edition SP2
- Microsoft SQL Server 2005 SP3
- Microsoft SQL Server 2008 SP1

Note that Websense Email Security currently supports only 32-bit SQL Server. Websense Email Security is a 32-bit application and cannot detect a 64-bit SQL Server during installation on a 64-bit Windows operating system.

Microsoft SQL Server 2008 Express is *not* supported for Websense Email Security version 7.2.

Although the v7.2 Personal Email Manager *Installation Guide* states otherwise, Personal Email Manager is no longer supported on Windows 2000 platforms.

Web browsers:

- Microsoft Internet Explorer version 6.0 SP1 or later
- Mozilla Firefox version 2.0 or later

Disk space recommendations:

For the Websense Email server machine:

- 4 GB random access memory (RAM) (2 GB minimum)
- 20 GB disk space (15 GB minimum)

Fixed issues

The issues described in this section have been corrected in Websense Email Security version 7.2.

Security fixes

This version of Websense Email Security includes 2 important security fixes:

- A remote distributed Denial of Services (DOS) vulnerability allowed remote attackers to disable the Websense Email Security Web Administrator service. This vulnerability has been fixed.
- A cross-site scripting (XSS) vulnerability in the Websense Email Security Web Administrator has been fixed.

> ✓ **Note**
> Special thanks to Nikolas Sotiriu from sotiriu.de for discovering these vulnerabilities and working with us through our disclosure program.

Rules Service

Some message attachments were corrupted when a Compress Attachment rule was used

This issue has been corrected.

Virus names were not always logged to the database depending on the Action object used in a rule

This issue has been corrected.

The number of Rules Service threads was not configurable for multiple Websense Email Security servers

This issue has been corrected.

Receive Service

Dynamic blacklist was not disabled when Directory Harvest Detection and Denial of Service were disabled

This issue has been corrected.

Personal Email Manager

Personal Email Manager treated the .eu domain as invalid

This issue has been corrected.

Personal Email Manager provided the JBoss status page to anyone who queried

This issue has been corrected.

Report Central

After database creation, the second of 2 sequential update tasks to different STEMLog databases did not complete

This issue has been corrected.

Release Notes additions

This section provides information about Websense Email Security v7.2 issues that became known after the product's release. Both issues involve the Configuration Wizard starting Websense Email Security services before database downloads are completed.

Unexpected error message during configuration

During Websense Email Security configuration, the following pop-up message may appear while the database download manager is running:

```
Failed to extract the compressed database file. The database
file might be used by Websense Email Security services.
Do you want to stop Websense Email Security Services?
```

This message appears because the Websense Email Security services start before the download manager completes its downloads. The Rules Service must be stopped for the proper extraction of the McAfee anti-virus database.

Click **Yes** in the pop-up window to stop the services and extract the McAfee database.

The Websense Email Security Configuration Wizard will restart the services.

Configuration Wizard timeout

During Websense Email Security v7.2 installation, the Configuration Wizard may experience the following timeout error while starting Websense Email Security services:

```
Error: Cannot start service: [service name]: This operation
returned because the timeout period expired.
```

The Configuration Wizard starts Websense Email Security services before the database download manager completes its downloads.

This timeout error may occur after the Anti-Virus Agent and Anti-Spam Agent have been downloaded. The Internet Threat Database may still be downloading.

Click **Retry** in the Configuration Wizard window for the wizard to start the services.