WEBSENSE®
Email Security

Administrator's Guide

Report Central

v2.7.2

©Copyright 2006-2009 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.

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 6,606,659 and 6,947,985 and other patents pending.

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.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

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:

Apache Tomcat

Copyright © 1999-2007, The Apache Software Foundation

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.

Commons Logging Version 1.1

Copyright 1999-2007 The Apache Software Foundation

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.

Java Activation Framework version 1.0

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

Java Advanced Imaging version 1.1.1

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

Java implementation of MD5

Copyright (c) 1998 - 2002, Paul Johnston & Contributors. All rights reserved.

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

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

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

Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

Sun JavaHelp API binaries

This product includes Sun JavaHelp API Binaries providing a full-featured, platform-independent, extensible help system. Java Help can be obtained from http://java.sun.com/products/javahelp.

Sun JavaMail API binaries

This product includes Sun JavaMail API Binaries providing a platform-independent and protocol-independent framework to build mail and messaging applications. JavaMail can be obtained from http://java.sun.com/products/javamail.

Java Mail version 1.3.1

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

JDBC Rowset

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

jRegistryKey - A JNI wrapper of the Windows Registry functions

Copyright (c) 2001, BEQ Technologies Inc.

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

jTDS JDBC Driver for Microsoft SQL Server and Sybase

Copyright © 2004 The jTDS Project

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Log4J

Copyright 1999-2005 The Apache Software Foundation.

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.

http://logging.apache.org/log4j/docs/index.html

OpenSSL encryption library version 0.973

Copyright © 1999-2009 The OpenSSL Project, All rights reserved.

Quartz version 1.6

Copyright © 2004-2005, The Apache Software Foundation

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.

Xerces Java Parser 1.4.4

This Product includes software developed by the Apache Software Foundation (http://www.apache.org/)

Copyright © 2000 The Apache Software Foundation. All right reserved.

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 License for Xerces Java Parser 1.4.4 can be found at: http://www.apache.org/licenses/LICENSE

Contents

1 Introduction

Welcome to Report Central, the reporting tool for Websense Email Security. Report Central generates custom reports that you design and standard reports created from templates. You can schedule reports to run and save reports in protected folders accessible only by selected users.

Report Central uses a SQL Server database for reporting that receives scheduled updates from the Websense Email Security database. Report administrators can manage the size of the reporting database by archiving and purging older data. Reports can be saved or exported to various formats and emailed to designated recipients.

Complete the following tasks to generate reports in Report Central:

Task 1: Configure your browser. See *Getting started*, page 7 and *Certificate management*, page 8 for details.

Task 2: Create user accounts and set permission levels. See *User accounts*, page 15 for details.

Task 3: Configure database linking. See *Database*, page 19 for details.

Task 4: Define settings for email notification. See *Mail settings*, page 30 for details.

Task 5: Schedule database maintenance tasks. See *Archiving or deleting reports*, page 30 for details.

Task 6: Select the reports you want to run. See *Drill-Down Manager*, page 35 and *Standard reports*, page 46 for details.

Task 7: Format and run your reports. See *Setting up reports*, page 57 and *Generating reports*, page 85 for details.

Task 8: Schedule and save reports as needed. See *Saving reports*, page 85.

Getting started

Before opening Report Central, configure your browser to allow pop-ups and cookies from the Report Central server. If you connect using HTTPS, the default security certificate generated by Report Central enables secure, encrypted communication; however, you can use a self-signed or Certificate Authority (CA) signed security certificate (see *Signed certificates from a Certificate Authority*, page 9).

Pop-up blockers

Configure your pop-up blocker to allow pop-ups from the Report Central server. If you are using Internet Explorer 6.0 or later:

1. Select **Tools** > **Pop-up Blocker** > **Pop-up Blocker Settings**.
2. Enter the URL of the Report Central server.
3. Click **Add**.

Cookies

Set your browser to allow cookies from the Report Central server. If you are using Internet Explorer 6.0 or later:

1. Select **Tools** > **Internet Options**.
2. In the Internet Options dialog box, select the **Privacy** tab, and then click **Sites**.
3. Enter the URL of the Report Central server.
4. Click **Allow**.

   The URL appears in the **Managed websites** field.
5. Click **OK**.

Certificate management

When a client attempts to access Report Central using HTTPS, the server sends a default digital security certificate to the browser that enables secure, encrypted communication. The browser displays the following Security Alert.

- Click **Yes** to use the default certificate for the duration of the Report Central session. The Security Alert is displayed at the start of each session.
- Click **View Certificate** to view and install the default certificate. The Security Alert is not displayed again until the certificate expires after 90 days.

After 90 days, the following security alert appears at the start of each session:

```
The security certificate has expired or is not yet valid.
```

If you use the default certificate, communications continue to be secure. To avoid triggering the Security Alert, you can do one of the following:

- Create and install a self-signed certificate, which you can renew regularly, usually yearly.
- Buy or obtain a valid, signed digital certificate from a Certificate Authority (CA).

  If you have your own CA server, you can use it to validate server and Virtual Private Network (VPN) certificates within your own network.

Report Central certificates are located in the **.sckeystore** file. This file is found in:

```
<Report Central installation folder>\Report Central\Tomcat\
```

Self-signed certificates

Prior to creating a self-signed certificate, ensure that the network is protected and the client and server are in the same domain.

To create a self-signed certificate:

1. Stop the Report Central service.
2. Open a command prompt, and then go to the following directory:

   ```
   <Report Central installation folder>\Report Central\Tomcat
   ```
3. To generate the certificate, valid for a period of 365 days, enter:

   ```
   ..\jre\bin\keytool -selfcert -alias tomcat -storepass changeit
   -validity 365 -keystore .sckeystore
   ```
4. Restart the Report Central service.

To install a self-signed certificate:

1. Select **Start** > **Programs** (or **All Programs**) > **Report Central** > **Email Security Reports – Secure Connection**

   This opens Report Central using HTTPS.
2. In the Security Alert that appears, click **View Certificate**.
3. Click **Install Certificate**.
4. Follow the instructions in the Install Certificate Wizard.
5. In the Security Alert, click **Yes**.

Repeat this procedure for each client.

Signed certificates from a Certificate Authority

To generate a Certificate Signing Request (CSR):

1. In a command prompt, go to the following directory:

   ```
   <Report Central installation folder>\Report Central\Tomcat
   ```

2. Enter the following command to create a file called **RC.txt**:

```
..\jre\bin\keytool.exe -certreq -keystore .sckeystore -file RC.txt
-alias tomcat
```

3. You are prompted for a password (**changeit** by default).
4. Send the newly created CSR file (**RC.txt**) to a Certificate Authority.

To import a signed certificate:

The response from the CA contains a file with a **.p7b** extension.

1. Stop the Report Central service.
2. Open a command prompt. Assuming the file is called **<filename>.p7b**, enter:

```
..\jre\bin\keytool.exe -import -trustcacerts -keystore .sckeystore
-alias tomcat -file <filename>.p7b
```

3. Enter a password when prompted. The default is **changeit**.

   A warning similar to the following appears:

   ```
   This certificate is not trusted. Install anyway?
   ```

4. Enter **Yes**.
5. Restart the Report Central service.

Passwords

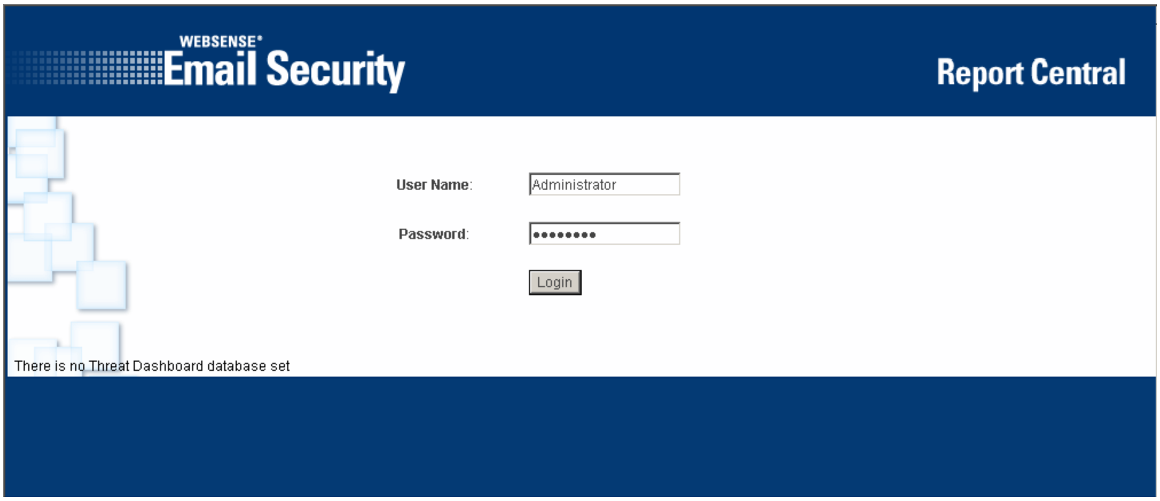
The passwords for the keystore and the private key are defaults and are not secure. It is good practice to change these passwords. See http://mindprod.com/jgloss/keytoolexe.html#PASSWORDS for details about changing the passwords. If the keystore password is changed, you must edit the Tomcat **server.xml** file to tell Tomcat the new password.

Opening Report Central

Use one of the following methods to open Report Central from the **Start** menu:

- To connect using HTTP, select **Programs** (or **All Programs**) > **Report Central** > **Websense Email Security Reports.**
- To connect using a secure connection with HTTPS, select **Programs** (or **All Programs**) > **Report Central** > **Websense Email Security Reports - Secure Connection.**

For details about the default security certificate and self-signed or Certificate Authority signed certificates, see *Certificate management*, page 8.



You can configure Report Central to display an overview of email traffic, called the Threat Dashboard, at the bottom of the logon screen. See *Database*, page 19 for configuration details. For a description of the Threat Dashboard and the information it displays, see *Threat Dashboard*, page 12.

Avoid security issues with Internet Explorer when you log on to Report Central by adding the URL of the Report Central server as a trusted site.

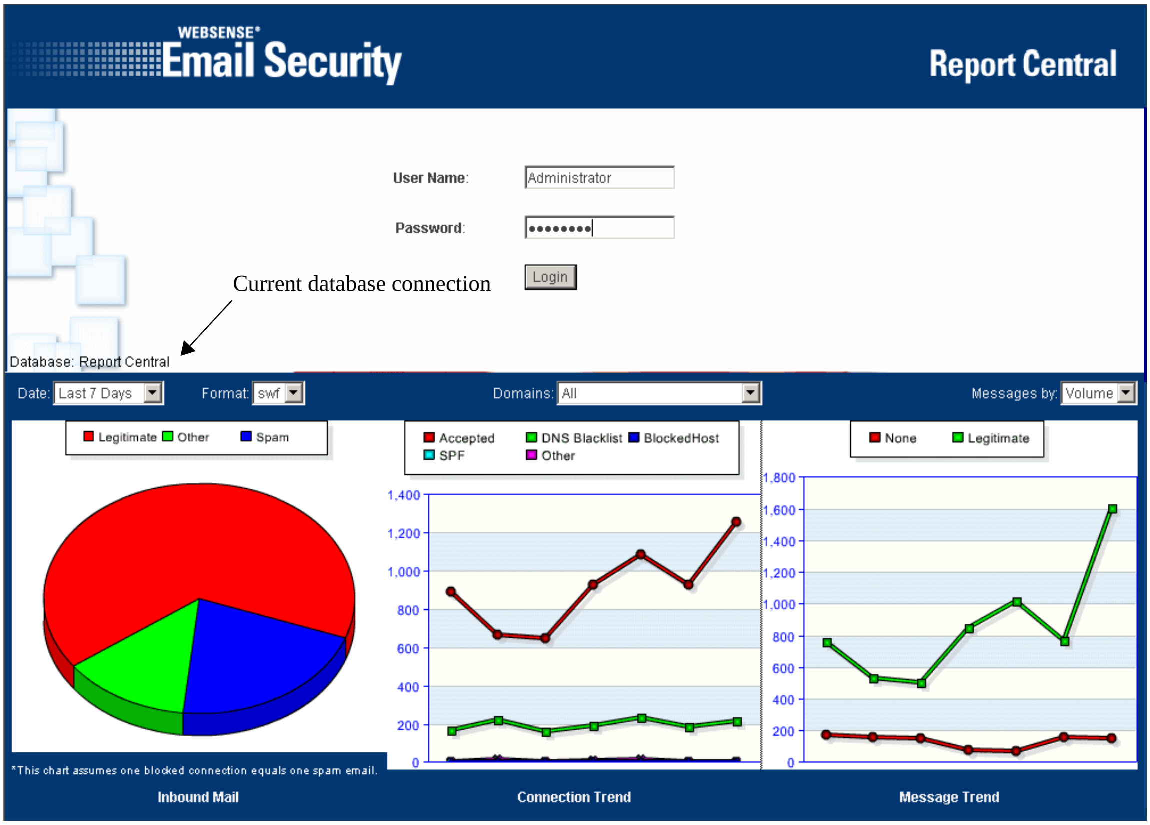
1. Select **Internet Explorer** > **Tools** > **Internet Options**.
2. Select the **Security** tab.
3. Select **Trusted Sites**, and then click **Sites**.
4. Enter the URL of the Report Central server, and then click **Add**.
5. Click **Close**, and then **OK** to exit Internet Options.

For your first login, enter the user name and password of the administrator you set up during installation. This user has Reports Administrator privileges.

If necessary, you can set up other users. See *User accounts*, page 15.

Threat Dashboard

The Threat Dashboard displays an overview of email traffic, as monitored in your current database. The name of the database connection is shown at the top of the dashboard.



Formatting

Use drop-down list boxes at the top of the dashboard to change the data that is shown and how it is displayed:

- **Date**: Select to show data from either the **Last 7 Days** or **Last 28 Days**.
- **Format**: Select a format for the dashboard display:
  - **.swf**: Macromedia Flash. You can install the free Flash viewer to view the dashboard in this format.
  - **.png**: Portable Network Graphic
  - **.jpg**: Joint Photographic Experts Group

  With the **png** and **jpg** formats, you can save the image, email it, or print the image from a right-click menu. You can include the graphs in reports or send them to an email distribution list.

- **Domains**: Select the domain to monitor or select **All**.
- **Messages by**: Sorting parameters for email messages. The choices are **Volume** and **Size**.

Data views

The Report Central dashboard shows the following details:

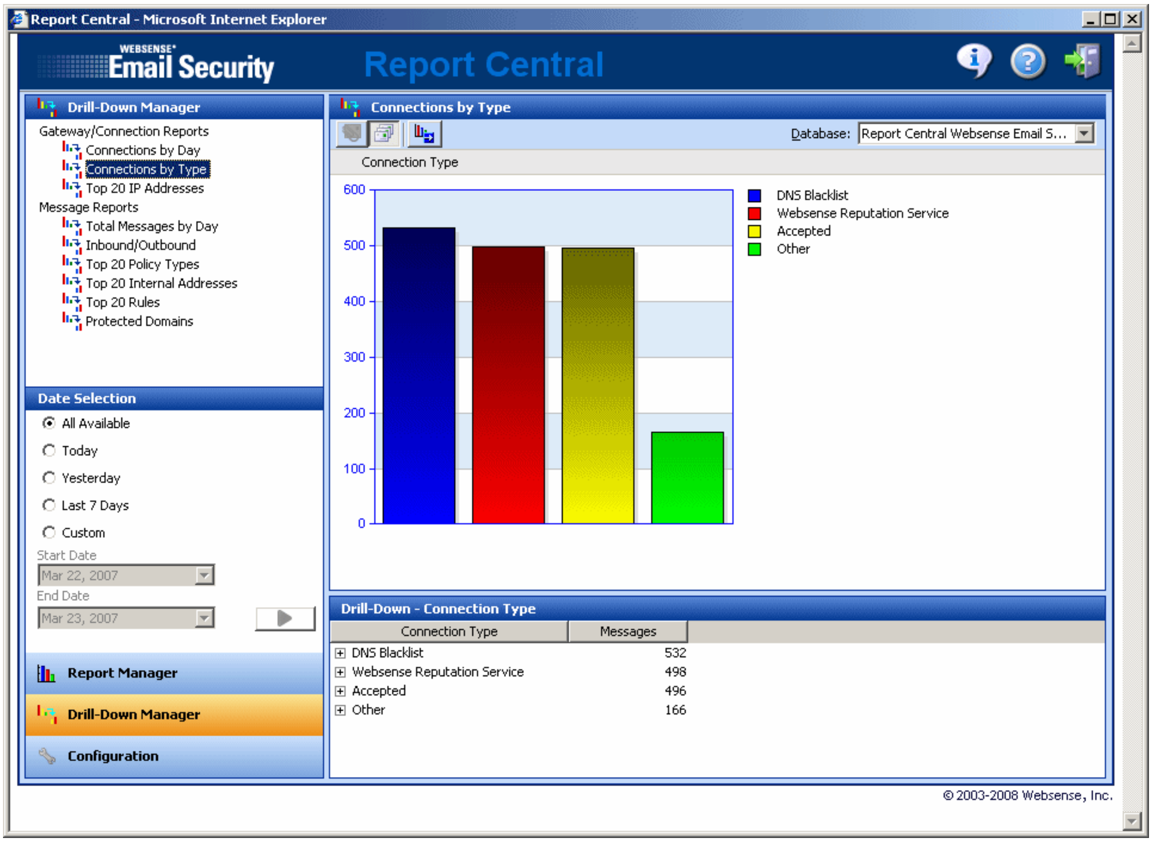
- **Inbound Mail**: Overall breakdown of inbound messages processed by Websense Email Security
- **Connection Trend**: Trend for the types of connections received at the gateway (such as Accepted, DHA, SPF, or DOS)
- **Message Trend**: Combined inbound and outbound trend for the types of email, as categorized by Websense Email Security (such as, Legitimate, Compliance, Spam, or Virus)

Report Central functions

When you log on to Report Central, the opening page displays data from the Drill-Down Manager. Use the controls in the lower left corner of the screen to access the following functions.

- **Configuration**: Set up users and database connections. See *Configuration*, page 15.
- **Drill-Down Manager**: Display data for a particular day or range of days. See *Drill-Down Manager*, page 35.
- **Report Manager**: Create and save reports for the data you need. See *Report Manager*, page 41.

The number of functions displayed depends on the privileges of the user.

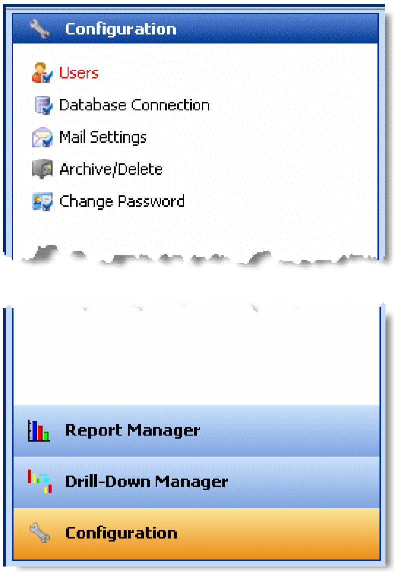


Report Central provides context-sensitive Help, including a full-text search facility and an index. Press **F1** or click the Help button. 

2 Configuration

The configuration options available depend on the type of user and the user's permissions. The possible options are:

- **Users**: Add, edit, and delete users. See *User accounts*, page 15.
- **Database Connection**: Create, edit, and delete database connections. See *Database*, page 19.
- **Mail Settings**: Set up a connection to your mail server to send reports by email. See *Mail settings*, page 30.
- **Archive/Delete**: Archive or delete your saved reports. See *Archiving or deleting reports*, page 30.
- **Change Password**: Change your own password. See *Changing passwords*, page 34.

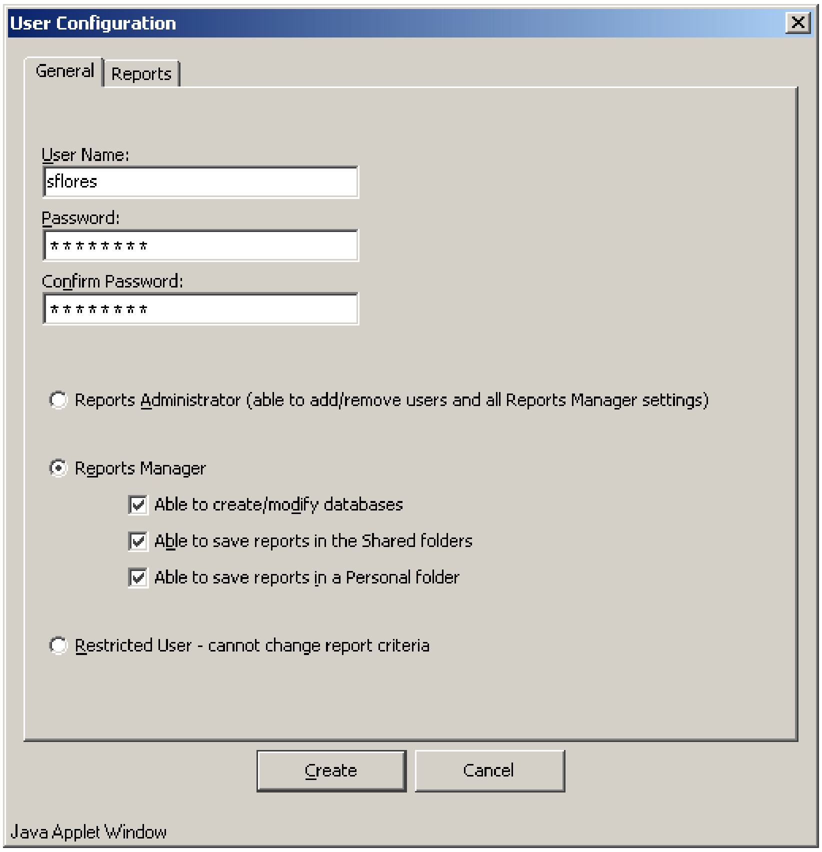


User accounts

User configuration sets the following account information:

- Logon details
- User permissions
- Report permissions

To access the user configuration options, select **Configuration** > **Users**, and then click **New**. The **User Configuration** dialog box appears.



Logon details

To configure logon details, select the General tab. Define a user name and password for your new user, and then define reporting permissions.

User access

There are three levels of reporting access:

- **Reports Administrator**: Create and edit users. The Administrator also has all Reports Manager privileges.
- **Reports Manager**: Has one or more of the following privileges:
  - Create and modify databases
  - Save reports in the Shared folders
  - Save reports in a Personal folder
- **Restricted User**: Run reports that have been set up by a Reports Administrator or Reports Manager. Restricted users cannot change the content of reports.

Changing the account for the Report Central service

If you change the user name or password for the Report Central service account, ensure that the user's access rights for the Report Central server and the SQL Server are correct.

1. Select **Start** > **Programs** (or **All Programs**) > **Administrative Tools** > **Services**

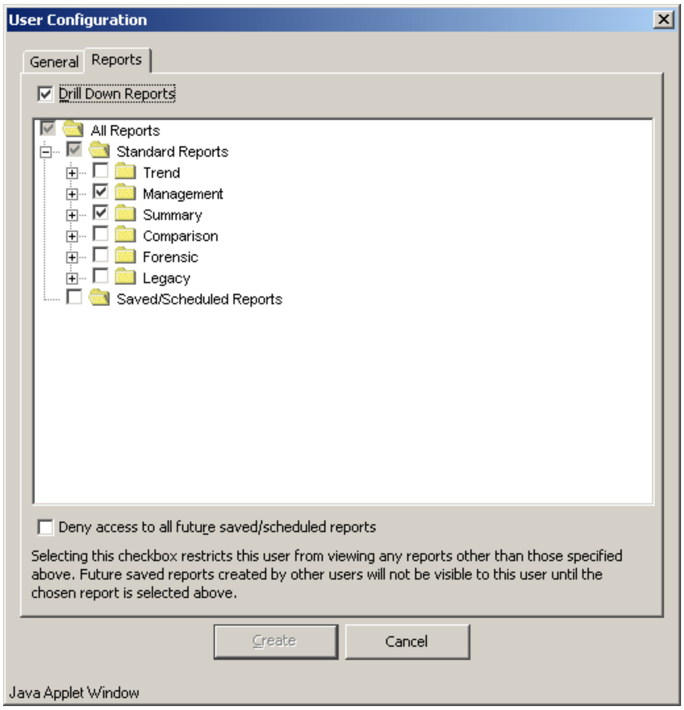
   The Services dialog box appears.
2. Right-click **Report Central Service**, and then select **Properties**.
3. In the Properties dialog box, select the **Log On** tab.
4. Enter a user name and a password.
5. Restart **Report Central Service**.

   You can now enter database connection details from Report Central.

Reporting permissions

There are four types of report permissions:

- Drill-Down Reports
- All Reports
- Standard Reports
- Saved/Scheduled Reports



Drill-Down reports

Drill-Down reports enable you to investigate the data on which a report is based. See *Drill-Down Manager*, page 35 for more details.

Standard reports

The following pre-configured, standard report templates are supplied with Report Central:

- Trend reports (see *Trend reports*, page 47)
- Management reports (see *Management reports—Return on Investment (ROI)*, page 47)
- Summary reports (see *Summary reports—Outbound Traffic*, page 51)
- Comparison reports (see *Comparison reports*, page 53)
- Forensic reports (see *Forensic reports*, page 54)
- Legacy reports (see *Legacy reports*, page 55)

For security, you can restrict a user's access to one or more report categories, or specific reports within categories. This ensures that only authorized users have access to specific reports.

For a detailed description of each category and report for Websense Email Security, see *Report Manager*, page 41.

Saved and scheduled reports

Authorized users can save reports and schedule reports to run. For details, see *Saving reports*, page 85. Reports can be saved in two types of folders:

- Shared: These reports can be run by any user who has the relevant permissions.
- Personal: These reports can be run and viewed only by the user who saved them.

Note

Shared and Personal folders are created within Report Central when a report is saved. They are not externally accessible.

Permission for creating Shared and Personal folders is granted to Reports Managers on the General tab of the User Configuration dialog box. For instructions, see *User access*, page 16.

For more details on saving reports, see *Saving reports*, page 85.

To grant user permission to run only certain saved reports:

1. Select **Configuration** > **Users**.
2. Select a user from the list of **Existing Users**.
3. Click **Edit**.

4. In the **User Configuration** dialog box, select the **Reports** tab.
5. Expand the tree under **Saved/Scheduled Reports**.
6. Select the check boxes of the desired reports.
7. If you want to limit the user's access to the existing saved reports only, select **Deny access to all future saved/scheduled reports**.
8. Click **OK**.

Changing user details

Users with Reports Administrator status can edit user details and delete user accounts.

1. Select **Configuration** > **Users**.
2. Select a user from the list of **Existing Users**.
3. Click **Edit**.

   The **User Configuration** dialog box shows the user's existing details. You can change all existing **General** and **Report** settings except for the **User Name**.
4. To delete a user, select that user from the list, and then click **Delete**.
5. Click **OK** to confirm your changes.

Database

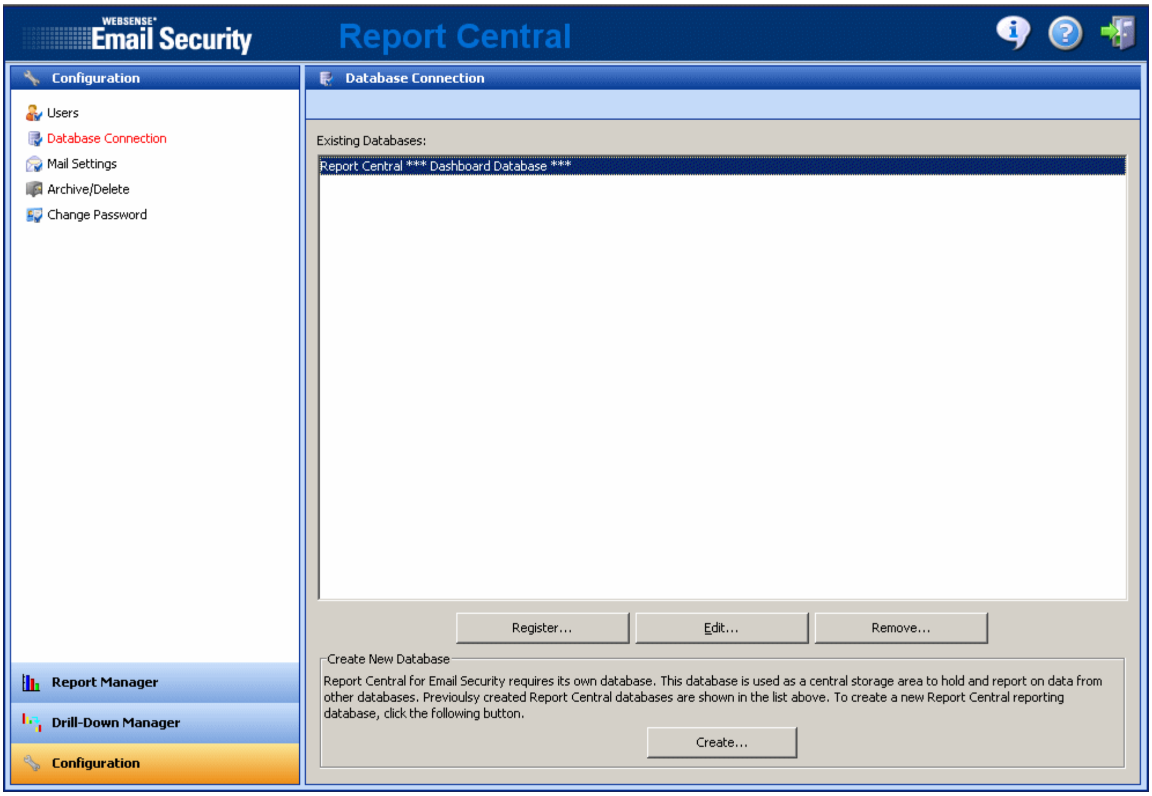
Report Central requires its own SQL Server database, which is used as a central storage area to hold and report on data from other databases. The Report Central database requires a linked server definition to the source Websense Email Security database to retrieve this data.

When you log on to Report Central for the first time, a database configuration wizard runs. Use this wizard to create or register a Report Central database and then link that database to the Websense Email Security database (see the Report Central *Installation Guide* for details).

To manage database connections, select **Configuration** > **Database Connection**.

From this screen, you can:

- Create a database.
- Register an existing database connection.
- Schedule database update tasks.
- Schedule database maintenance tasks.
- Configure the Threat Dashboard to appear on the logon page.



Database recommendations

- **Database free space**: Space needed on the Report Central database to receive data from a Websense Email Security database during an update

  Allow for 1.5 times as much free space as the size of the Websense Email Security database. For example, if the Websense Email Security database size is 60 GB, make the free space allotment 90 GB.

- **Update interval**: Time interval between automated database update tasks for the Report Central database

  For small databases (approximately 50,000 email messages), allow 5 minutes. For a larger database, allow 10 minutes.

  If the time between tasks is set too low, the next task attempts to start, but fails. The following error is logged in the **scheduler.log** file and shows the linked server, source catalog, and the database display name.

  ```
  Failed scheduled database update...
  ```

  This error does not affect the performance of your system, but indicates that you should increase the interval between the database update tasks. It is good practice to check the log file regularly for this error.

Adding database connections

To report on a new database, add the database connection details to the list. The following users can add a database connection:

- Reports Administrator
- Reports Manager with the **Able to change/modify databases** privilege

Adding a new database connection is a two-part procedure.

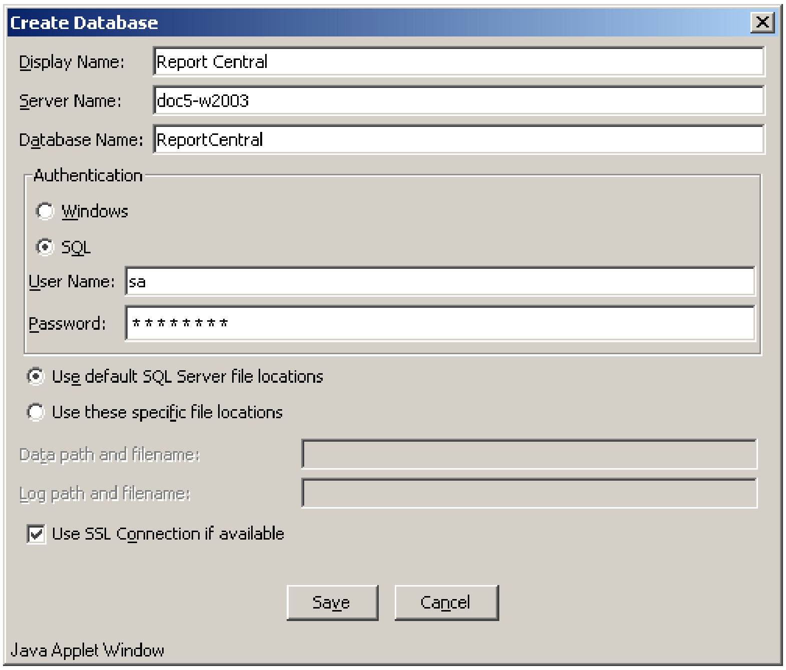
1. Add a connection to the database with one of the following procedures:
   - Create a new database. See *Creating a database for Websense Email Security reports*, page 21.
   - Register an existing database. See *Registering a database*, page 22**.**
2. Schedule update tasks. See *Schedule database updates*, page 24.

> **Note**
> To manage the size of your database, schedule regular archiving and purging tasks. See *Database maintenance*, page 28.

Creating a database for Websense Email Security reports

1. Select **Configuration** > **Database Connection**.
2. Click **Create.**

   The Create Database dialog box appears.



3. Identify the Report Central database server.

- **Display Name**: Display name of the Report Central database. This name is shown in the main Database Connection screen in Report Central and not in SQL Server
- **Server Name**: Machine name or IP address of the Report Central server
- **Database Name**: Name of the SQL Server database that you want to create. This is the name of the database as it appears in SQL Server.

4. Select an **Authentication** method for the Report Central server database.
    - **Windows**: Recommended authentication method

    > **Important**
    > Windows authentication is not supported if SQL Server is installed on a remote machine *and* you selected **Local System Account** for your Report Central service.

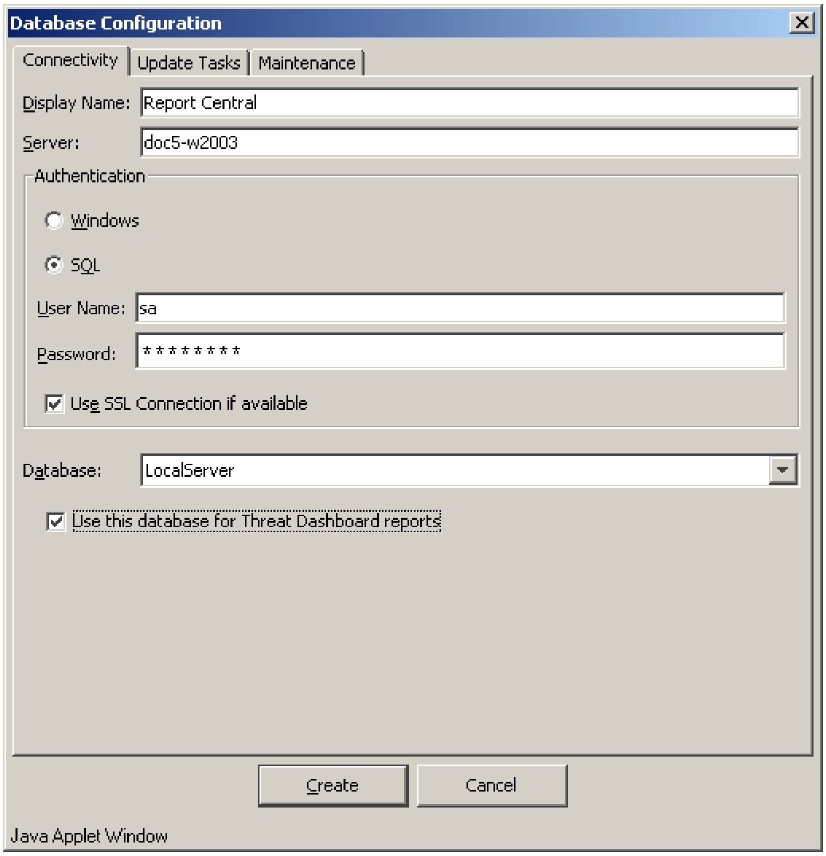
    - **SQL**: Enter the user name and password of a SQL Server account with SQL Server administrator rights.
5. Provide location information for SQL Server files.
    - **Default SQL Server file locations**: Select this if the files were installed in the default SQL Server location.
    - **Use these specific file locations**: Enter a preferred path for the **Data File** and **Log File**. Use this selection if you are creating a new Report Central database.
6. To use a secure connection for the Report Central database, select **Use SSL Connection if available**.
7. Click **Save**.

Registering a database

To register a database connection:

1. Select **Configuration** > **Database Connection**.

2. In the Database Connection screen, click **Register**, and then select the Connectivity tab.



3. Identify the Report Central database server.
   - **Display Name**: Name of the Report Central database. This is shown in the main Database Connection screen in Report Central.
   - **Server Name**: Machine name or IP address of the Report Central database server
4. Select an **Authentication** method for the Report Central server database.
   - **Windows**: Recommended authentication method.

> **Important**
> Windows authentication is not supported if SQL Server is installed on a remote machine *and* you selected **Local System Account** for your Report Central service.

   - **SQL**: Enter the user name and password of a SQL Server account with SQL Server administrator rights.
5. To use a secure connection for the Report Central database, select **Use SSL Connection if available**.
6. From the drop-down list box, select the database with which to connect.

7. To use the information from this database for the reports viewed from the logon screen, select **Use this database for Threat Dashboard reports**.

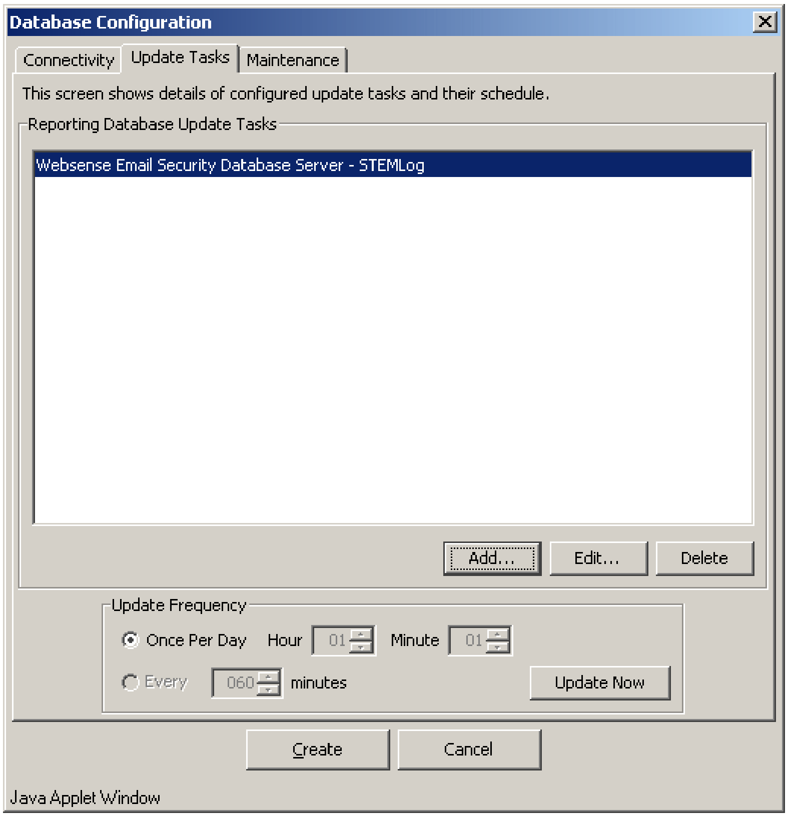
> **Note**
> Only one database can be used at a time for the Threat Dashboard display.

8. Click **Create**.

   For information about scheduling database updates, see *Schedule database updates*, page 24.

Schedule database updates

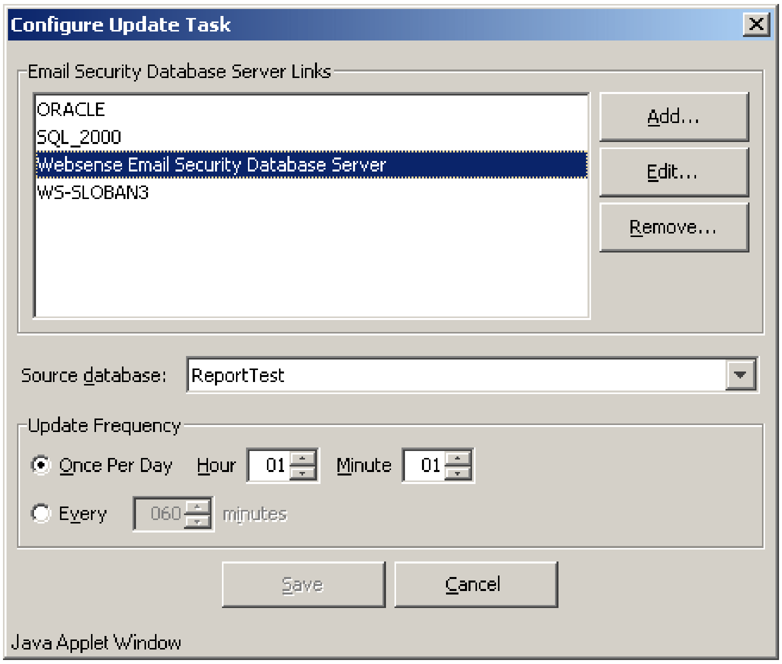
Use the Update Tasks tab to set the scheduling of Report Central database updates for a specific database connection. You can view the scheduling details for existing Update Tasks in this tab or click **Update Now** to update the database manually.



Editing update tasks

1. To edit an update task, select the Websense Email Security database, and then click **Edit**.

   The Configure Update Task dialog box appears. The database connection from the Update Tasks tab is selected.



2. Edit the update frequency.

   Time is expressed in a 24-hour clock.

   - **Once Per Day**: It is good practice to schedule updates for a time when Websense Email Security database activity is light.
   - **Every <*n*> minutes**: Define a sensible interval for your system. Frequent updates on a busy system can slow performance.

Important

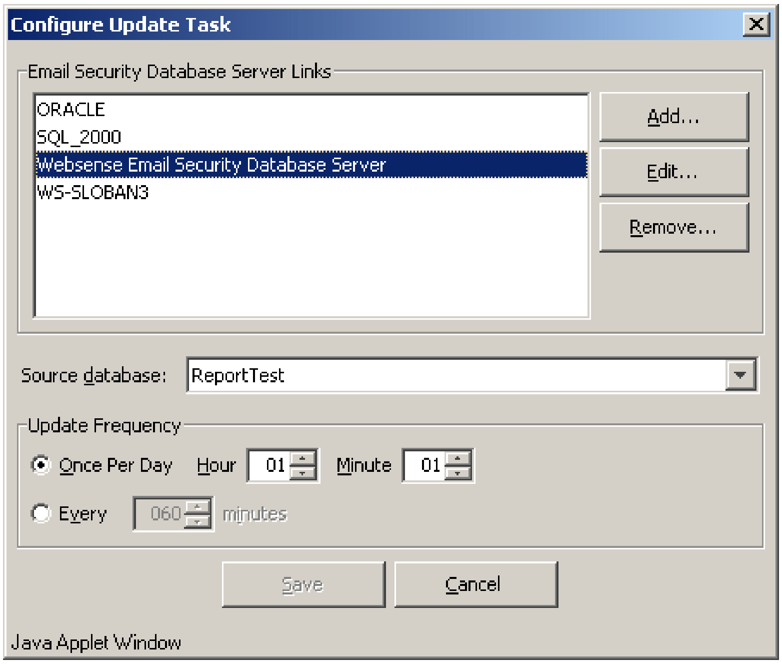
Run this update once per day to ensure that drill-down reports show accurate information. Make sure the update does not conflict with any other database maintenance tasks.

3. Click **Save**.

Adding update tasks for existing database connections

1. To add an update task for an existing Websense Email Security database connection, click **Add**.

   The Configure Update Task dialog box appears.



2. Select a Websense Email Security database link from the list.
3. Define an update frequency.

   Time is expressed in a 24-hour clock.

   - **Once Per Day**: It is good practice to schedule updates for a time when Websense Email Security database activity is light.
   - **Every <*n*> minutes**: Define a sensible interval for your system. Frequent updates on a busy system can slow performance.

Important

Run this update once per day to ensure that drill-down reports show accurate information. Make sure the update does not conflict with any other database maintenance tasks.

4. Click **Save**.

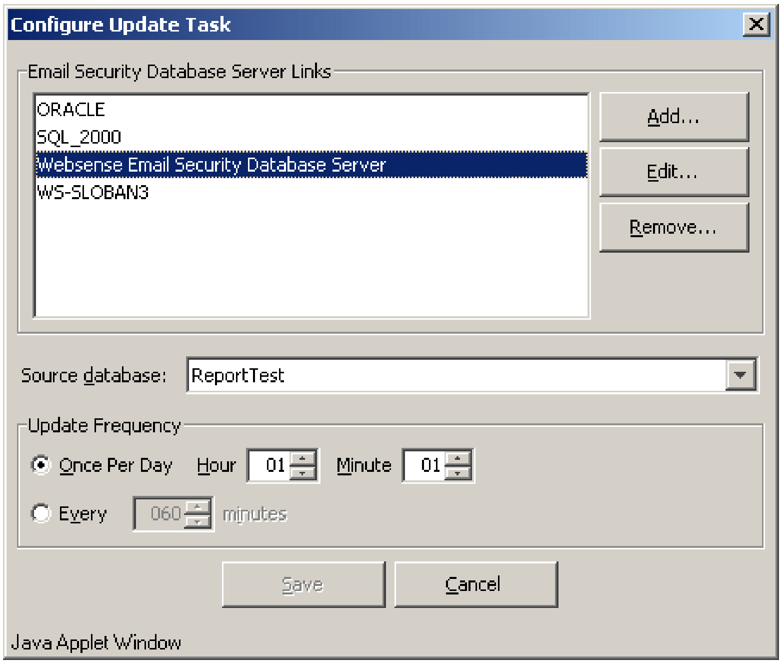
   The new link appears in the list in the Update Tasks tab.

Adding update tasks for new database connections

You can create new Websense Email Security database connections, and then add update tasks.

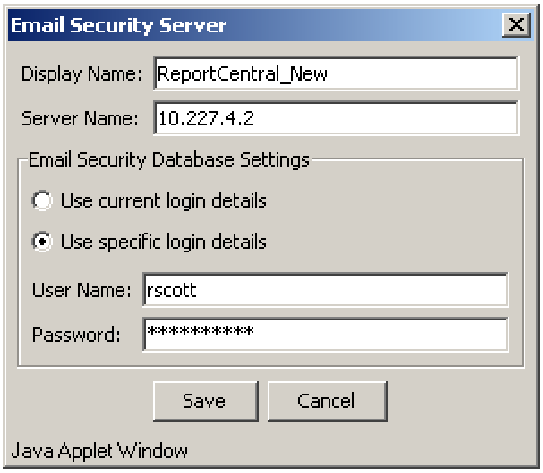
1. To create a new Websense Email Security database connection with an update task, click **Add**.

   The Configure Update Task dialog box appears.



2. Click **Add** to create the new database definition.

   The Email Security Server dialog box appears with all the fields enabled.



- **Display Name**: Display name as you want it to appear in the Update Tasks tab
- **Server Name**: Machine name or IP address of the SQL Server machine running the Websense Email Security database
- **Database Settings**: Logon details for this server

3. Click **Save** to create the definition.
4. Define an update task for your new database server link, and then click **Save**.

   The database and server name are displayed in the **Reporting Database Update Tasks** list in the Update Tasks dialog box.

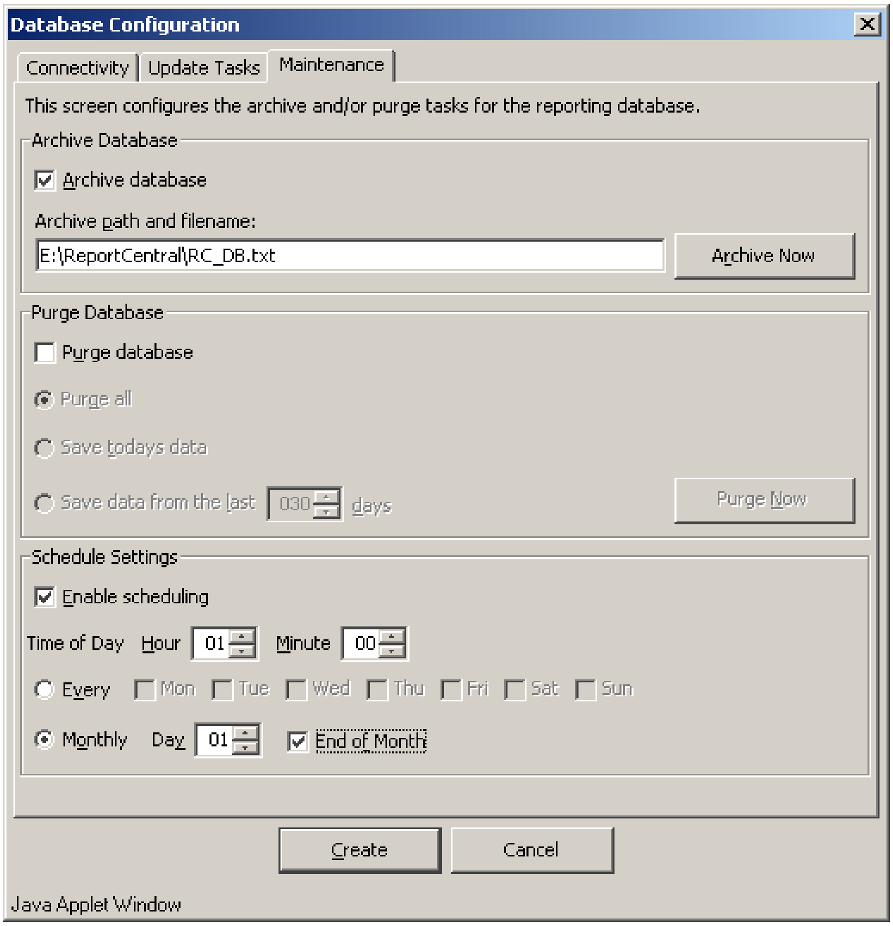
Editing an existing database connection

1. To edit the settings for an existing Websense Email Security database definition, click **Edit** in the Update Tasks tab.
2. Select a database definition from the list in the Configure Update Tasks tab.
3. Click **Edit**.

   The Email Security Server dialog box appears. The **Display Name** and **Server Name** fields are read-only, showing the specifics of the connection you selected in the previous dialog box.
4. Edit the logon details for this server.
5. Click **Save**.

Database maintenance

Select the Maintenance tab to schedule database archiving and purging tasks.



1. Select **Archive Database** to enable data archiving.
2. Enter the path to the archive folder, including a file name.
3. Click **Archive Now** to manually archive the data to the file named.
4. Select **Purge Database** to enable the purging selection.

   Database purge options are:

   - **Purge all**
   - **Save today's data**
   - **Save data from the last <*n*> days**
5. Click **Purge Now** to manually purge the database according to the selection you have made.
6. Click **Enable Scheduling** to create a schedule for both the archiving and purging tasks you selected.

   The default start time is 00:00 (24-hour clock). At this time, the scheduler starts the database maintenance tasks. It is good practice to run database maintenance when network traffic is light. The data is archived first, and then purged.

   > **Important**
   > Make sure you do *not* schedule database archive or purge tasks to run at the same time as the Report Central database update.

7. Click **Create** to save your selections.

Database update log files

Database update log files are stored in the **scheduler.log** file. This file is found in:

```
<Report Central installation folder>\Report
Central\Tomcat\webapps\EmailSecurity
```

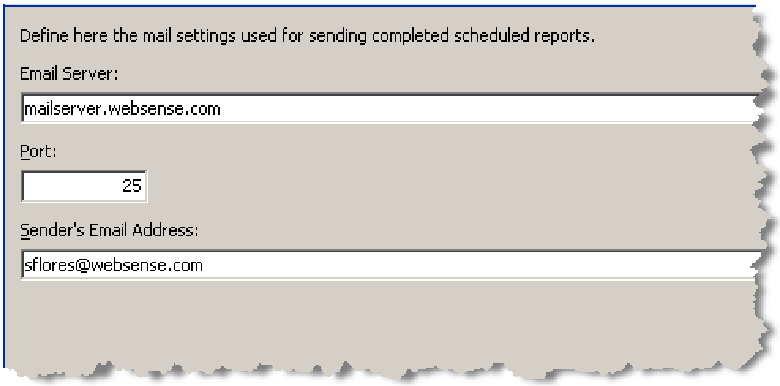
Logs include the following details:

- Start and end time of each scheduled update task
- Any failures of the task
- Retry attempts. If the task fails, it has up to 3 more attempts before it fails completely.

Mail settings

Use the Mail Settings in the Configuration page to identify your mail server. Users cannot send reports by email until this is done.

1. Select **Configuration** > **Mail Settings**.



2. In the **Email Server** field, enter the name of the mail server to be used to distribute reports.

   An example is, **mailserver.mycompany.com**
3. In the **Port** field, enter the number of the port to be used to send outbound email, usually port 25.
4. In the **Sender's Email Address** field, enter the email address from which to send reports.

   For example, **reportadmin@mycompany.com**
5. Click **Apply**.

Archiving or deleting reports

You can specify how Report Central deals with reports that are no longer current. Decide which reports are to be deleted or archived and decide when this should occur.

Enabling report archiving and deletion

To delete or archive reports, enable the archive and delete facility.

1. Select **Configuration** > **Archive/Delete**.
2. Select **Enable Deletion and Archiving**.

   By default, the **Delete Reports** option is enabled.
3. To enable the archive settings, select the **Archive Reports** option.

   You are now ready to set the properties for each.

Deleting reports

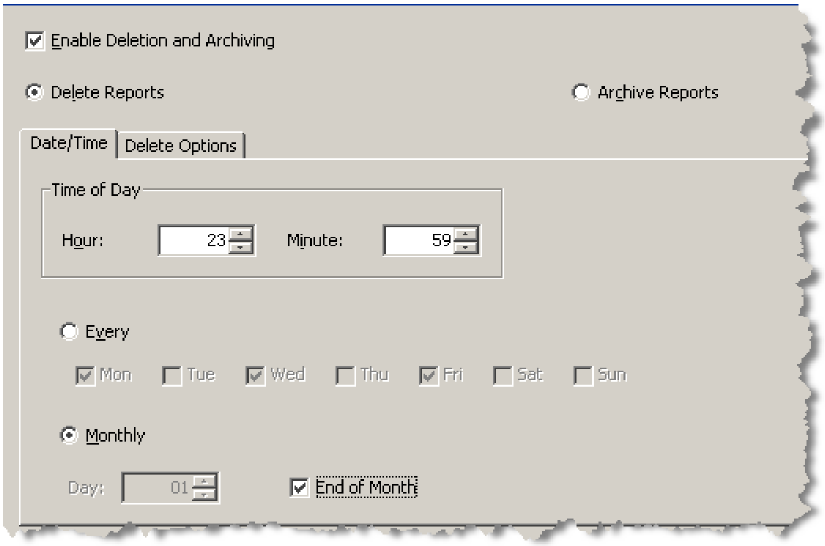
Decide which reports to purge in the Delete Options tab.

1. Select **Configuration** > **Archive/Delete**.
2. Ensure that the **Enable Deletion and Archiving** check box is selected, and then select **Delete Reports**.
3. Select the Delete Options tab.

4. Select one of the options:
   - All (the default setting)
   - Before today
   - Older than last 7 days
   - Older than last full month

To schedule a delete option:

1. Select the **Date/Time** tab.



2. Specify the **Time of Day** (24-hour clock) to delete your reports.
3. Select the day on which to delete the reports:
   - To delete reports on certain days of the week, select **Every**, and then select the relevant check boxes.
   - To delete reports on a specific day of the month, select **Monthly**, and then change the **Day** field.
   - To delete reports on the last day of each month, select **End of Month**.
4. Click **Apply**.

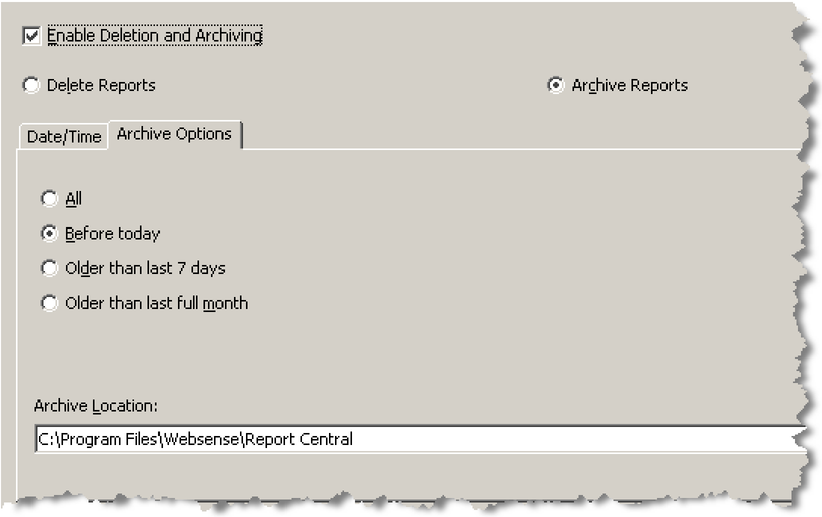
Archiving reports

Use the **Archive Reports** feature to schedule archiving by the age of the reports.

> **Note**
> Reports are archived individually in their original format.

1. Select **Configuration** > **Archive/Delete**.
2. Ensure that **Enable Deletion and Archiving** is selected, and then select **Archive Reports**.

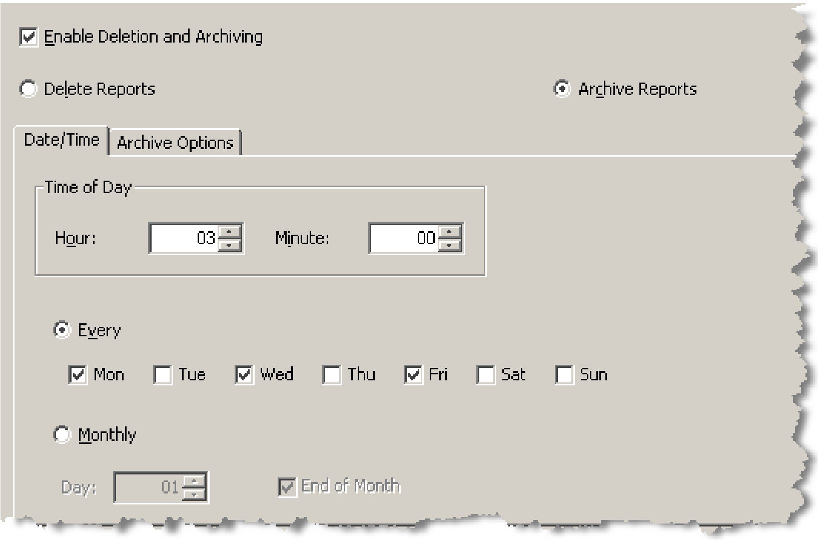
3. Select the Archive Options tab.



4. Select one of the options:
   - All (the default setting)
   - Before today
   - Older than last 7 days
   - Older than last full month
5. In the **Archive Location** field, specify a folder in which to store the archived reports.

To schedule archiving:

1. Select the **Date/Time** tab.



2. Specify a **Time of Day** (24-hour clock) to archive your reports.
3. Select archiving by day or month.
4. Click **Apply**.

Changing passwords

Users can change their own passwords.

1. Select **Configuration** > **Change Password**.
2. Enter a new password, and then confirm it.
3. Click **Apply**.

A Reports Administrator can also change the password of other users.

1. Select **Configuration** > **Users**.
2. Select a user from the list that appears.
3. Click **Edit**.
4. In the General tab, enter a new password, and then confirm it.

   See *Changing user details*, page 19.

Scheduler log

A log file (**Scheduler.log**) is created for all scheduled events, with the exception of summary data refreshed between scheduled updates. The default installation folder for the log file is:

```
<Report Central installation folder>\Report
Central\Tomcat\webapps\EmailSecurity
```

3 Drill-Down Manager

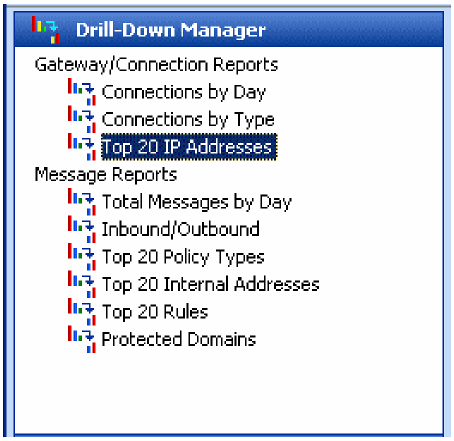
Use Drill-Down reports to investigate the data from which a report is generated. Drill-Down report data is updated on a daily basis. The timing of these updates can be scheduled in the Update Tasks tab in the Database Configuration screen. See *Schedule database updates*, page 24 for more details.

> **Note**
> Only permitted users have access to Drill-Down Reporting. See *User access*, page 16 for more details.

The Drill-Down Manager page is split into the following panes:

- Report selection
- Date selection
- Report view
- Drill-down data

Selecting reports

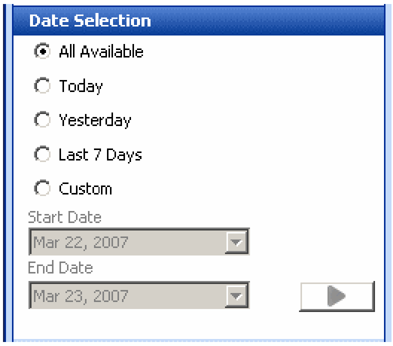


Select the reports you want to view from the Drill-Down Manager pane.

The available reports are:

- Gateway/Connection Reports:
  - Connections by Day (the default report view)
  - Connections by Type
  - Top 20 IP Addresses
- Message Reports:
  - Total Messages by Day
  - Inbound/Outbound
  - Top 20 Policy Types
  - Top 20 Internal Addresses
  - Top 20 Rules
  - Protected Domains

Selecting dates

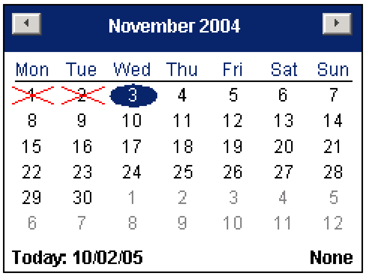


1. Select specific dates for the report view from the Date Selection pane.

   The options are:

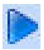
   - All Available
   - Today
   - Yesterday
   - Last 7 Days (the default view)
   - Custom

   When you select **Custom**, the **Start Date** and **End Date** fields are enabled.



2. Click in either date field to display a calendar.

   Dates crossed off in red are not available for selection.

3. When you have specified start and end dates, click **Go.** 

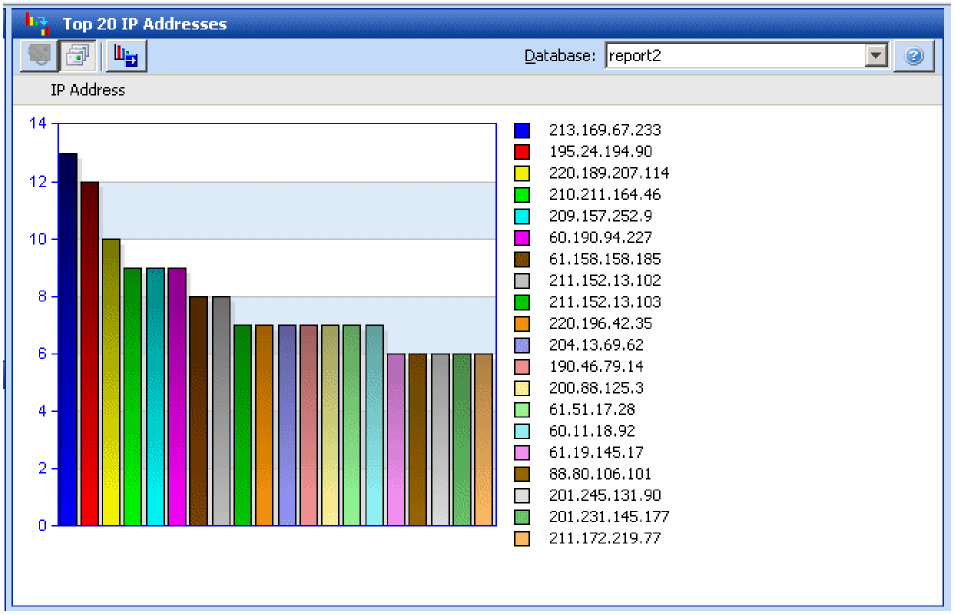
Note
For **All Available** and **Custom** date ranges encompassing more than 31 days of data, refer to the Drill-Down Data pane for the complete date range. The graph in the Report View displays data for the last 31 days only.

Report view

The report view pane displays reports by:

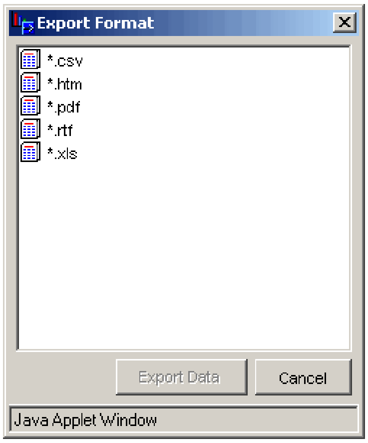
- Message size (including attachments) 
- Number of messages (volume) 

Use the **Database** drop-down list at the top of the screen to select other configured database connections. For information on database connections, see *Database*, page 19.



Exporting report data

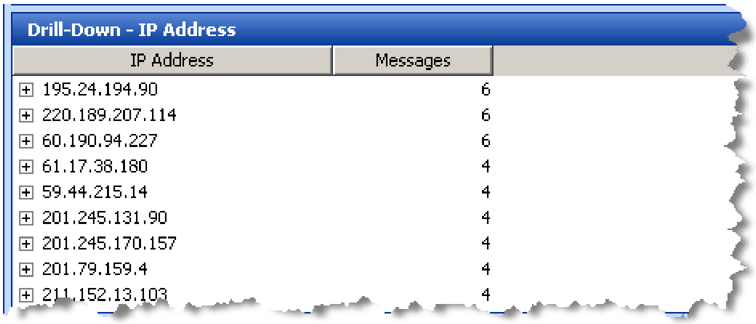
To export the report data, click the **Export Data** icon,  and then select a format from the **Export Format** dialog box.



- ***.csv**: For use in spreadsheet or database programs, such as Microsoft Excel or Microsoft Access
- ***.htm**: For viewing with a Web browser
- ***.pdf**: For viewing with a portable document format viewer, such as Adobe Acrobat
- ***.rtf**: For use with a word processor, such as Microsoft Word
- ***.xls**: For use with Microsoft Excel (version 8 or later)

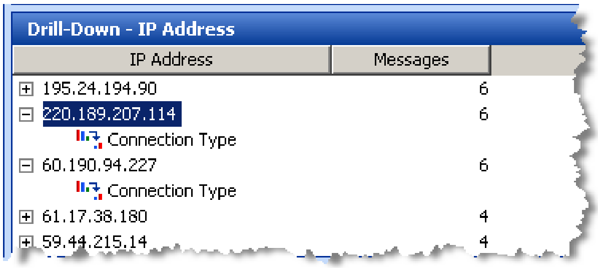
Drill-down data

The drill-down data displayed varies according to the report selected and whether you are viewing by Size or Volume. The initial view displays a collapsed view of the report data tree.



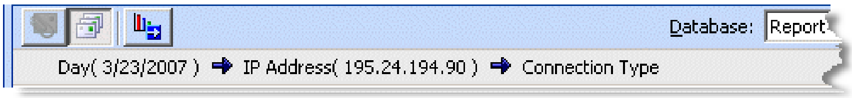
Navigating drill-down data

Expand a category to view the drill-down data in sub-categories. These sub-categories are hyperlinks to the data.



The graph in the Report View pane displays the selected data.

A navigation strip (breadcrumbs) above the graph helps you move backward and forward through the data. Each step is a hyperlink that takes you back to a previous step in the drill-down process.



4 Report Manager

You can generate two types of reports in the Report Manager:

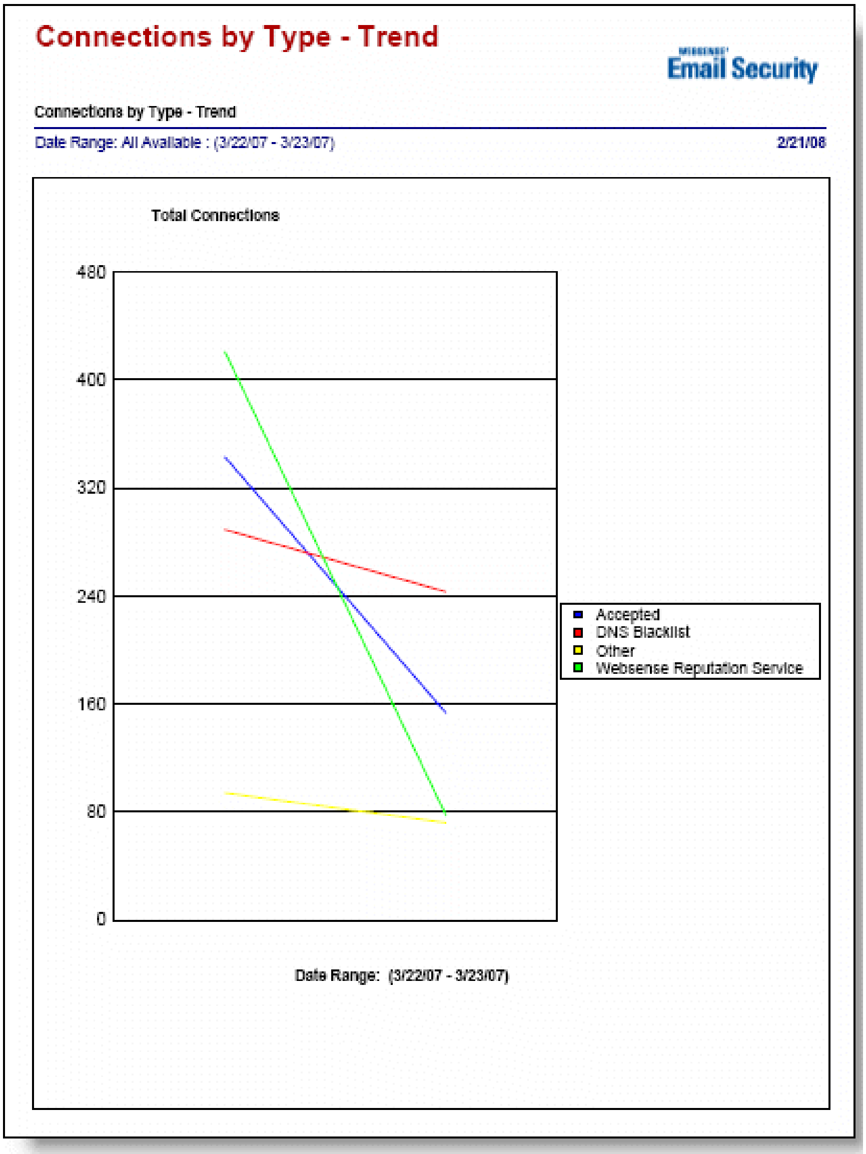
- **Standard Reports**: Reports generated from supplied settings (criteria). See *Standard reports*, page 46 for descriptions of each report template.
- **Saved/Scheduled Reports**: Reports generated using your own saved settings. For details, see *Schedule settings*, page 83 and *Saving reports*, page 85.

Report display formats

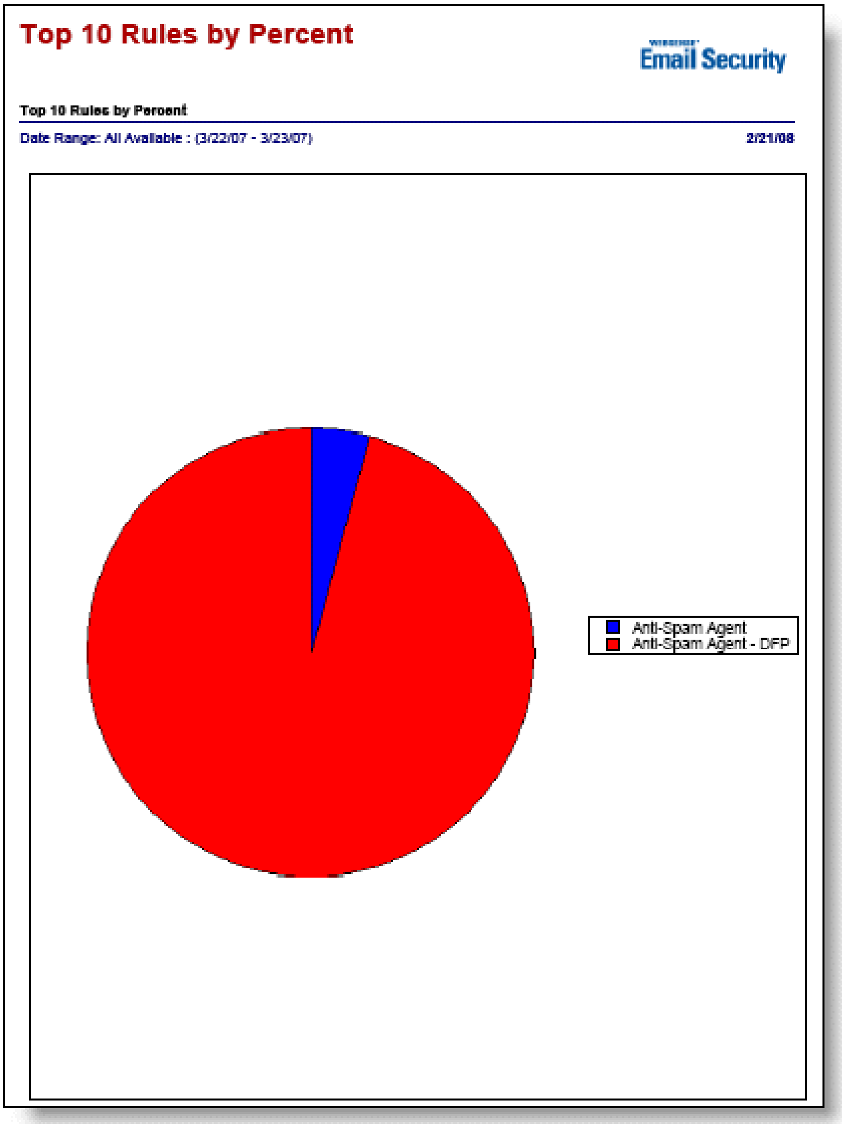
Some reports are displayed as tables, others are displayed as charts. The types of formats available are:

- Line plot
- Pie chart
- Bar chart – horizontal
- Bar chart – horizontal (split)
- Table

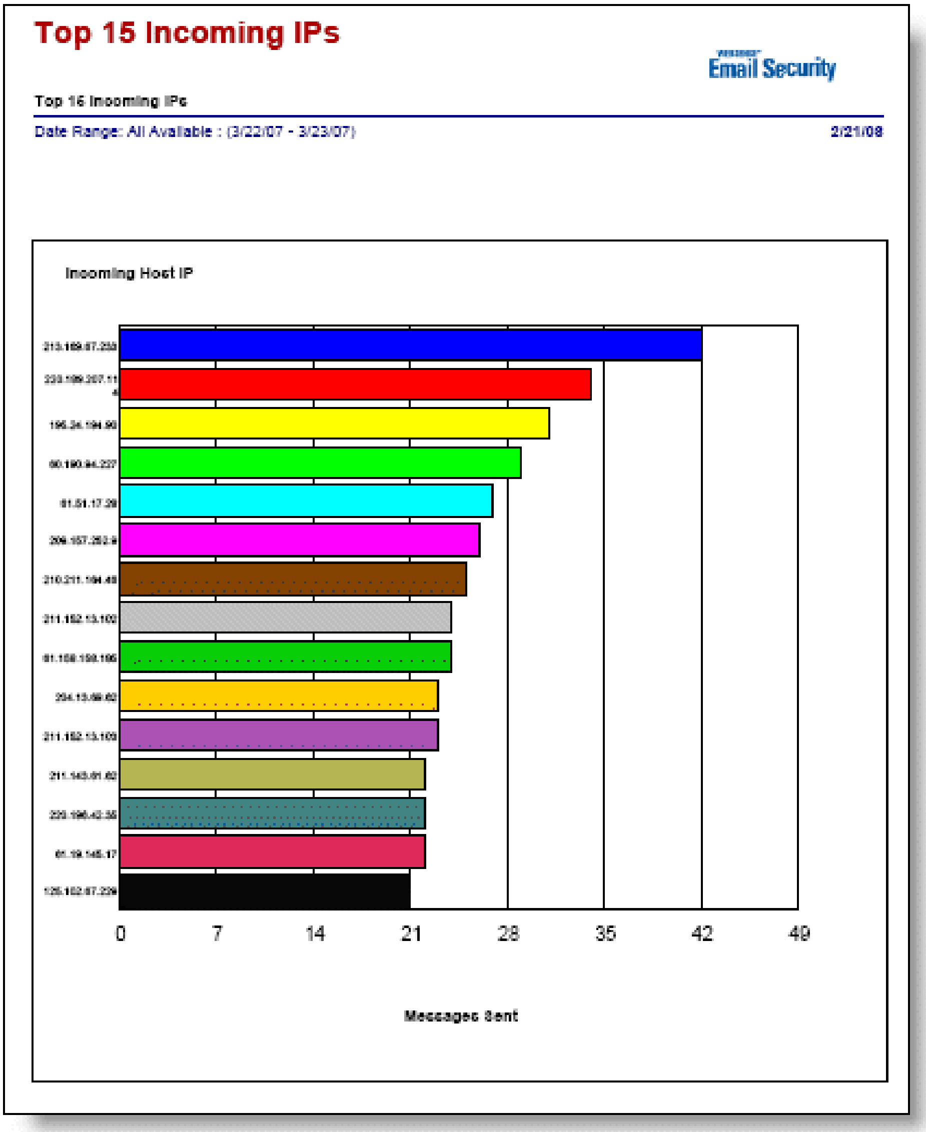
Line plot


Connections by Type - Trend
Email Security
Connections by Type - Trend
Date Range: All Available : (3/22/07 - 3/23/07)
2/21/08
Total Connections
480
400
320
240
160
80
0
Accepted
DNS Blacklist
Other
Websense Reputation Service
Date Range: (3/22/07 - 3/23/07)

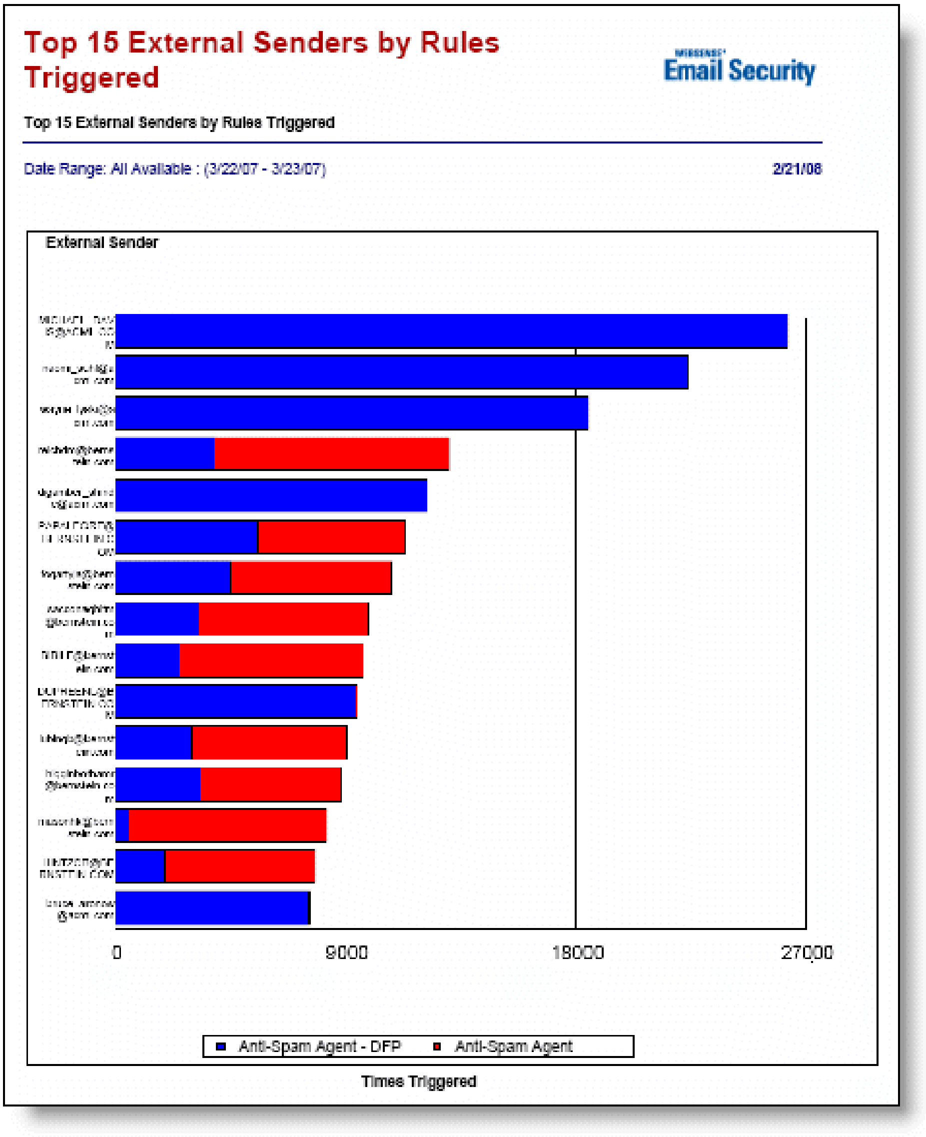
Pie chart


Top 10 Rules by Percent
Email Security
Top 10 Rules by Percent
Date Range: All Available : (3/22/07 - 3/23/07)
2/21/08
Anti-Spam Agent
Anti-Spam Agent - DFP

Bar chart – horizontal



Bar chart – horizontal (split)



Table

Rules by Sender - Details

Email Security

Rules by Sender - Details

Date Range: All Available : (3/22/07 - 3/23/07) 2/21/08

This report is restricted to 20000 records. You can reduce the number of records returned by selecting specific criteria.

Sender	Rule	Date/Time	Action	Recipient
079538044-0001@t-online.de				
	Anti-Spam Agent - DFP	3/23/07 3:27:42 AM	Isolate	webmaster@alpharelease.com
aadk.xope@msa.hinet.net				
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	sindia@hotels.com.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	pilot@imeifoods.com.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	mine0830@iris.seed.net.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	midst@mail.sysnet.net.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	pennyn01@ms15.hinet.net
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	peng1206@ms18.hinet.net
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	mystic_17_82@ms64.hinet.net
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	osh0798@ms24.hinet.net
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	richpaul@ms34.hinet.net
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	kgo0928045511@yahoo.com.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	l3085s@yahoo.com.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	miik20042002@yahoo.com.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	miki52120@yahoo.com.tw
	Anti-Spam Agent - DFP	3/23/07 2:49:50 AM	Isolate	mm26797498@yahoo.com.tw

1

Standard reports

All standard reports use **Date/Time** criteria to create the report. By default, reports are based on all available criteria and data for the last 7 days. For details of available criteria that you can change to create reports, see *Report criteria*, page 60.

All reports contain the Date Range and the date on which the report was run. The data shown depends on the type of report.

- Trend (*Trend reports*, page 47)
- Management:
  - Return on Investment (*Management reports—Return on Investment (ROI)*, page 47)
  - Connection Based (*Management reports—Connections*, page 47)
  - Traffic Based (*Management reports—Traffic*, page 48)
- Summary:
  - Inbound Traffic (*Summary reports—Inbound Traffic*, page 49)
  - Outbound Traffic (*Summary reports—Outbound Traffic*, page 51)
- Comparison (*Comparison reports*, page 53)
- Forensic (*Forensic reports*, page 54)
- Legacy (*Legacy reports*, page 55)

Trend reports

Report Name	Type	Data Shown	Report Criteria
Connections by Type – Trend	• Line plot • Pie chart	• Connection Type • Total Connections	• Date/Time • Options
Messages by Type – Trend	• Line plot • Pie chart	• Total Messages • Number of Connections	• Date/Time • Options • Protected Domain

Management reports—Return on Investment (ROI)

The following table describes the content of the Return on Investment (ROI) report. This report has only Date/Time and Options criteria, both of which are used to create the report.

This report uses the specified cost of a single occurrence of a spam email or virus entering your organization. Virus and spam costs are configurable. See *Options*, page 79 for more information.

Report Name	Type	Data Shown	Report Criteria
Return on Investment	• Pie chart • Bar chart – horizontal, tables	• Details of total inbound email messages • Number of email messages blocked at connections level • Number of email messages blocked by spam rules • Cost savings from spam protection • Cost savings from virus protection	• Date/Time • Options

Management reports—Connections

Report Name	Type	Data Shown	Report Criteria
Connections by Type – Summary	Pie chart	• Connection Type • Total Connections	• Date/Time • Connection Type • IP Address

Report Name	Type	Data Shown	Report Criteria
Top 15 Connections	Bar chart – horizontal	• IP Address • Accepted Connections	• Date/Time • Connection Type • IP Address
Top N Connections by Type	Table	• Connection Type • IP Address • Total Connections	• Date/Time • Options • Connection Type • IP Address

Management reports—Traffic

Report Name	Type	Data Shown	Report Criteria
Message Traffic by Action	Pie chart	• Date • Message Action[1] • Total Messages	• Date/Time • Protected Domain • Policy Type
Message Traffic by Type	Pie chart	• Date • Policy Type • Total Messages	• Date/Time • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top 10 Rules by Percent	Pie chart	• Rule • Total Triggered • Percentage	• Date/Time • Protected Domain
Top N Incoming IPs	Bar chart – horizontal	• Incoming Host IP • Host Name • Number of Messages Sent • Volume	• Date/Time • Options • Protected Domain
Top N Internal Addresses	Bar chart – horizontal (split)	• Address • Inbound • Total Messages	• Date/Time • Options • Protected Domain • Policy Type
Top N Rules Triggered	Bar chart – horizontal	• Rule • Times Triggered	• Date/Time • Options
Top N Viruses	• Bar chart – horizontal • Table	• Virus • Total viruses	• Date/Time • Protected Domain • Options

1. An entry of **Manual** for the **Message Action** indicates that a manual action on the email, such as **Release**, has been carried out in Websense Email Security Message Administrator or Personal Email Manager. For more information, see the *Administrator's Guide* for each of these products.

Summary reports—Inbound Traffic

Report Name	Type	Data Shown	Report Criteria
Inbound Message Traffic by Type	Pie chart	• Policy Type • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top 10 Rules Triggered by Percentage of Received Messages	Bar chart – horizontal	• Rule • Times Triggered • Percentage	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top 15 External Senders by Rules Triggered	Bar chart – horizontal (split)	• Rule • Sender • Times Triggered	• Date/Time • Options • Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N External Senders by Total Size	Bar chart – horizontal	• Sender • Total Size (KB)	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type

Report Name	Type	Data Shown	Report Criteria
Top N External Senders by Total Volume	Bar chart – horizontal	• Sender • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Recipients by Total Size	Bar chart – horizontal	• Recipient • Total Size (KB)	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Recipients by Total Volume	Bar chart – horizontal	• Recipient • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N IPs by Rule	Table	• Incoming Host IP • Host Name • Rule • Times Triggered	• Date/Time • Options • Internal Address • Protected Domain • IP Address • External Domain • External Address • Day of Week • Rule Name • Policy Type

Report Name	Type	Data Shown	Report Criteria
Top N Rules by IPs	Table	• Rule • Incoming Host IP • Host Name • Times Triggered	• Date/Time • Options • Internal Address • Protected Domain • IP Address • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N Rules Triggered by Received Messages	Bar chart – horizontal	• Rule • Times Triggered	• Date/Time • Options • Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type

Summary reports—Outbound Traffic

Report Name	Type	Data Shown	Report Criteria
Outbound Message Traffic by Type	Pie chart	• Policy Type • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top 10 Rules Triggered by Percentage of Sent Messages	Bar chart – horizontal	• Rule • Times Triggered • Percent	• Date/Time • Options • Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type

Report Name	Type	Data Shown	Report Criteria
Top 15 Internal Senders by Rules Triggered	Bar chart – horizontal (split)	• Internal Sender • Rule • Times Triggered	• Date/Time • Options • Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type
Top N External Recipients by Total Size	Bar chart – horizontal	• Recipient • Total Size (KB)	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N External Recipients by Total Volume	Bar chart – horizontal	• Recipient • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Senders by Total Size	Bar chart – horizontal	• Sender • Total Size (KB)	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Top N Internal Senders by Total Volume	Bar chart – horizontal	• Sender • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type

Report Name	Type	Data Shown	Report Criteria
Top N Rules Triggered by Sent Messages	Bar chart – horizontal	• Rule • Times Triggered	• Date/Time • Options • Internal Address • IP Address • Protected Domain • External Domain • External Address • Day of Week • Rule Name • Policy Type

Comparison reports

Report Name	Type	Data Shown	Report Criteria
Message Traffic by Date	Bar chart – horizontal (split)	• Date • Inbound • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Policy Type
Message Traffic by Hour	Bar chart – horizontal (split)	• Hour • Inbound • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week • Policy Type
Message Traffic by Weekday	Bar chart – horizontal (split)	• Day of Week • Inbound • Total Messages	• Date/Time • Options • Internal Address • IP Address • Protected Domain • External Domain • External Address

Forensic reports

Report Name	Type	Data Shown	Report Criteria
Message History	Table	• Internal Address • Date/Time • Direction • External Address • Subject • Number of Attachments [1] • Rule Triggered	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Messages by Size	Table	• Message Size • Sender • Date/Time	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Rules by Date	Table	• Rule • Date • Sender • Recipient • Subject	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Rules by Sender – Details	Table	• Sender • Rule • Date/Time • Action • Recipient	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type

Report Name	Type	Data Shown	Report Criteria
Rules by Sender – Summary	Table	• Sender • Rule • Total Messages • Total Size (KB)	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type
Rules by Sender Showing Recipient	Table	• Sender • Rule • Date • Recipient • Subject	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Rule Name • Direction • Policy Type

1. A blank entry in the Attachments column indicates that Report Central could not determine if the email contained attachments.

Legacy reports

Report Name	Type	Data Shown	Report Criteria
Top 10 Rules by Percent	Bar chart – horizontal	• Rule • Total Triggered • Percentage	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Recipients by Total Messages	Bar chart – horizontal	• Recipient • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week

Report Name	Type	Data Shown	Report Criteria
Top 15 Recipients by Total Size	Bar chart – horizontal	• Recipient • Total Size	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Rules	Bar chart – horizontal	• Rule • Total Messages	• Date/Time • Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Percent	Bar chart – horizontal	• Sender • Total Messages • Percent	• Date/Time • Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Rules Triggered	Bar chart – horizontal	• Sender • Rule • Number of Times Triggered	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Total Messages	Bar chart – horizontal	• Sender • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week
Top 15 Senders by Total Size	Bar chart – horizontal	• Sender • Total Size	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week

Report Name	Type	Data Shown	Report Criteria
Top N Incoming IPs	Bar chart – horizontal	• IP Address • Total Messages	• Date/Time • Options • Internal Address • Protected Domain • External Domain • External Address • Day of Week

Setting up reports

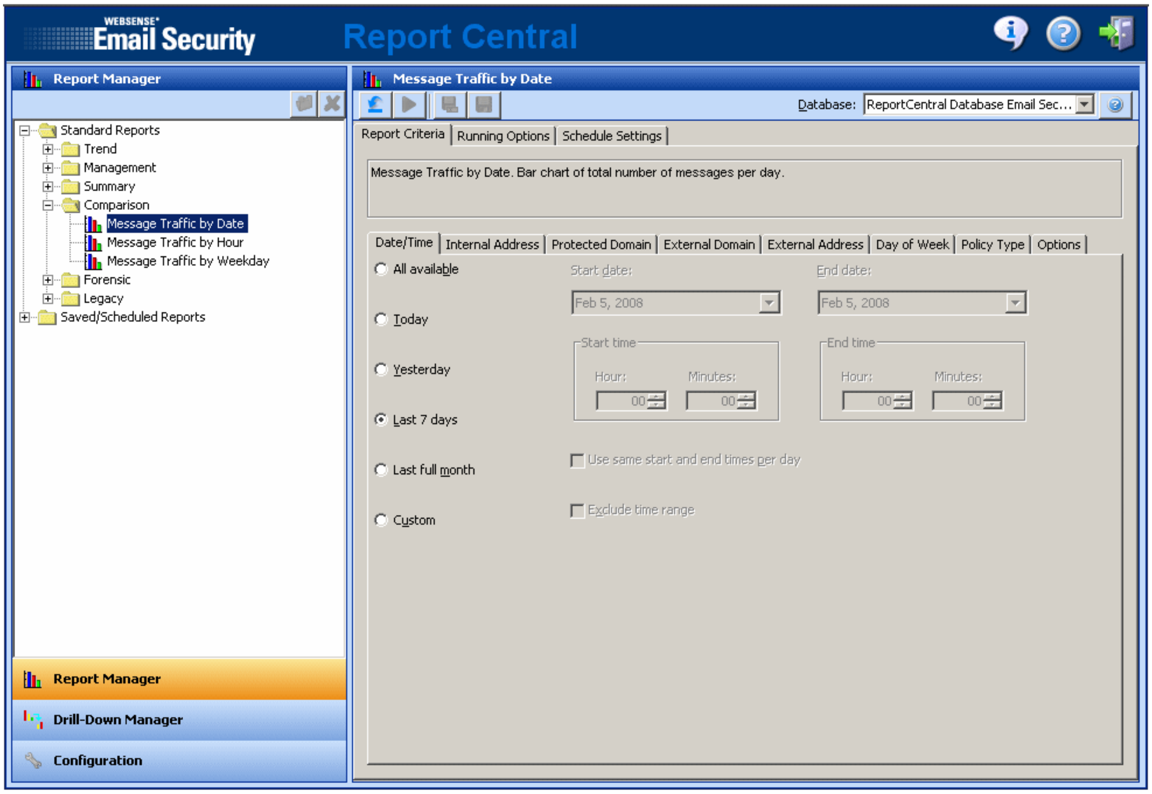
There are four steps to setting up a report:

1. Select the report you want to run.
2. Specify report criteria.
3. Specify running options.
4. Specify scheduling options.

Once a report has been scheduled and saved, the Report History tab appears in the Report Manager, providing details about the report. See *Report history*, page 59 for details.

Selecting a report

From the **Report Manager** pane, select a report from one of the categories. The criteria for that report are displayed as tabs in the right-hand pane.



Important

Make sure the time and date on the Report Central machine and the SQL Server machine are the same. If these do not match, the time and date may not be reported accurately.

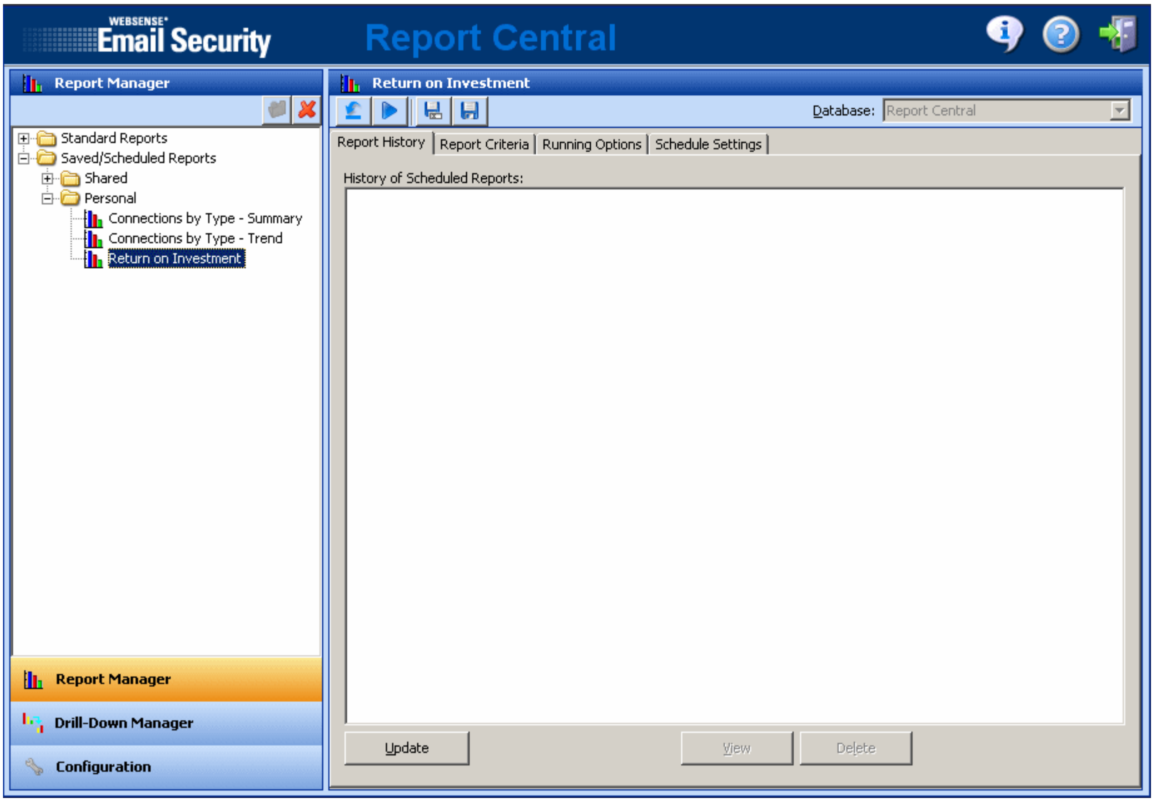
When you select a report, Report Central retrieves the time and date information from the database. If there is a problem connecting to your database, you receive an error message detailing the problem.

Check for the following:

- Report Central is connecting to a valid Websense Email Security database (**Configuration** > **Database Connections**).
- The Websense Email Security database to which Report Central is connected contains valid data.
- SQL Server is running correctly.

Report history

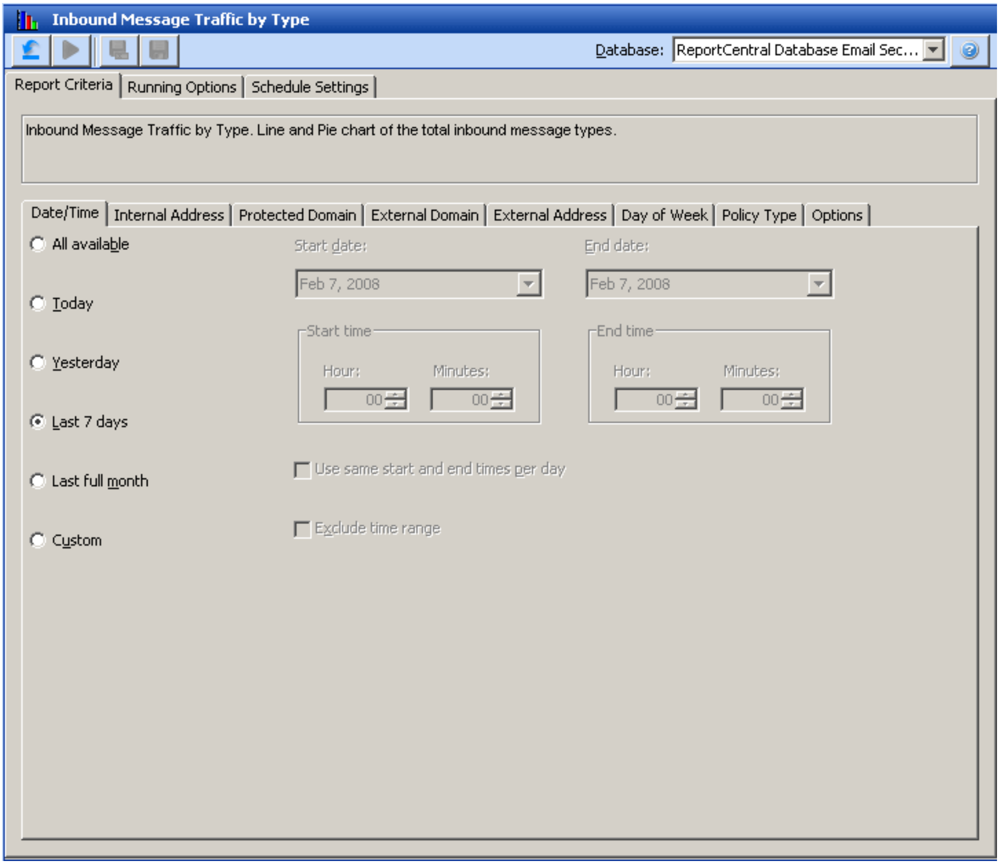
When a scheduled report has been run and saved, it is displayed in the **Report History** tab in the Report Manager. To view the history of a report, expand the tree beneath **Saved/Scheduled Reports** and then again under either **Shared** or **Personal**. Select the report to display the history in the tab.



> **Note**
> If this tab is open when the report is run, the report is not shown in the list. Click **Update** to display the report.

Report criteria

Use the options in the Report Criteria tab to select various details for your report. The criteria available to you depend on the type of report you select and your user permissions.



Available criteria are:

- Date/Time: Available for all reports. See *Date/Time*, page 61.
- Connection Type: Available only for connection-based Management reports. See *Connection Type*, page 62.
- IP Address: See *IP Address*, page 63.
- Internal Address: See *Internal Address*, page 65.
- Protected Domain: See *Protected Domain*, page 67.
- Rule Name: Available for Forensic and some Summary reports only. See *Rule Name*, page 69.
- External Domain: See *External Domain*, page 71.
- External Address: See *External Address*, page 73.
- Day of Week: See *Day of Week*, page 75.
- Policy Type: See *Policy Type*, page 76.
- Direction: Available only for Forensic reports. See *Direction*, page 78.

- Options: Available for all reports. See *Options*, page 79.

The save options on the Report Criteria tab are:

- Revert to the last saved report settings (or the default).
- Save the settings to a different report name.
- Save to replace the default settings (available only for saved reports).

For details about the save options, see *Saving reports*, page 85. If you do not use any of the save options, your settings are discarded when you log off Report Central.

Date/Time

The following table shows the Date/Time criteria.

Date/Time	Description
All Available	All available data stored on the database
Today	Data logged to the database today (between 00:00 and the last database update)
Yesterday	Data logged to the database yesterday (between 00:00 and 24:00)
Last 7 Days	Data logged to the database in the last seven days (the default setting)
Last full month	Data logged to the database in the last full month
Custom	Data logged to the database in the time period you specify

Custom time period

Use this option to report on data from a time period that you specify.

1. Click in the **Start Date** drop-down list box and select a day from the calendar.

> **Note**
> Dates crossed off in red on the calendar are not available for selection.

2. Click in the **End Date** drop-down list box and select a day from the calendar.
3. Specify a **Start Time** and an **End Time** (24-hour clock).
4. To report on data from the same time period each day, select **Use same start and end times per day.**

   See *Standardized daily time period*, page 62 for details.
5. To report on data from outside the time period you specify, select **Exclude Time Range.**

   See *Exclude time range*, page 62 for details.

Standardized daily time period

Select the **Use same start and end times per day** option to report on data from the same time frame each day.

Checkbox	Action	Example
Cleared	This report uses data from the entire date range you specify, beginning at the start time on the start date and ending at the end time on the end date.	Between 0900 on day 1 and 1700 on day 3
Selected	Report Central uses report data from the time period you specify, for each day between the start and end date.	Between 0900 and 1700 on day 1, 0900 and 1700 on day 2, etc.

Exclude time range

You can use the **Exclude Time Range** check box independently of the **Use same start and end times per day** check box.

Checkbox	Action	Example
Cleared	The report uses data from the time period you specify.	Between 0900 and 1700 on day 1
Selected	The report uses any data excluded by the **Use same start and end times per day** options.	Midnight until 0900 and 1700 until 2359 on day 1

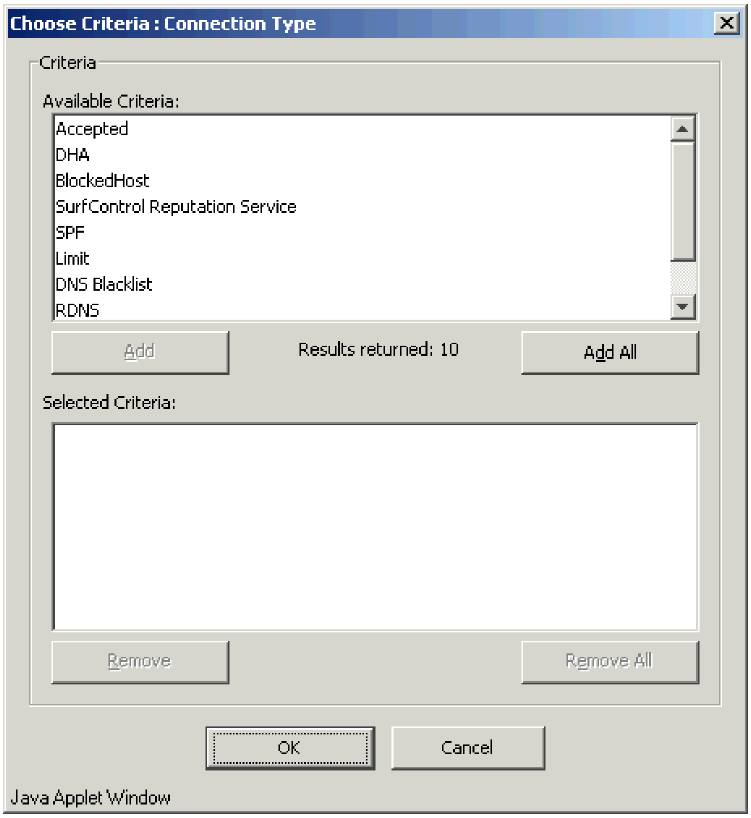
Connection Type

Use this tab to include or exclude connection types, such as Accepted, Blocked Host, DNS Blacklist, or RDNS.

1. Select the **Connection Type** tab.
2. To include all connection types in the report, select **Include all**.
3. To include or exclude connection types from the report, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add connection types.
   - If the Selected Criteria list contains connection types, the view does not change. Click **Add** to add connection types to the list, or click **Remove** to delete connection types.



4. Select connection types from the **Available Criteria** list, and then click **Add**.
5. Click **Add All** to add all connection types from the availability list.

   The selected connection types are displayed in the **Selected Criteria** list.
6. To remove connection types from the **Selected Criteria** list, select the connection type, and then click **Remove**. To remove all connection types from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for connection types.

7. Click **OK**.

   The connection types are added to the **Selected Criteria** list in the **Connection Type** tab.

IP Address

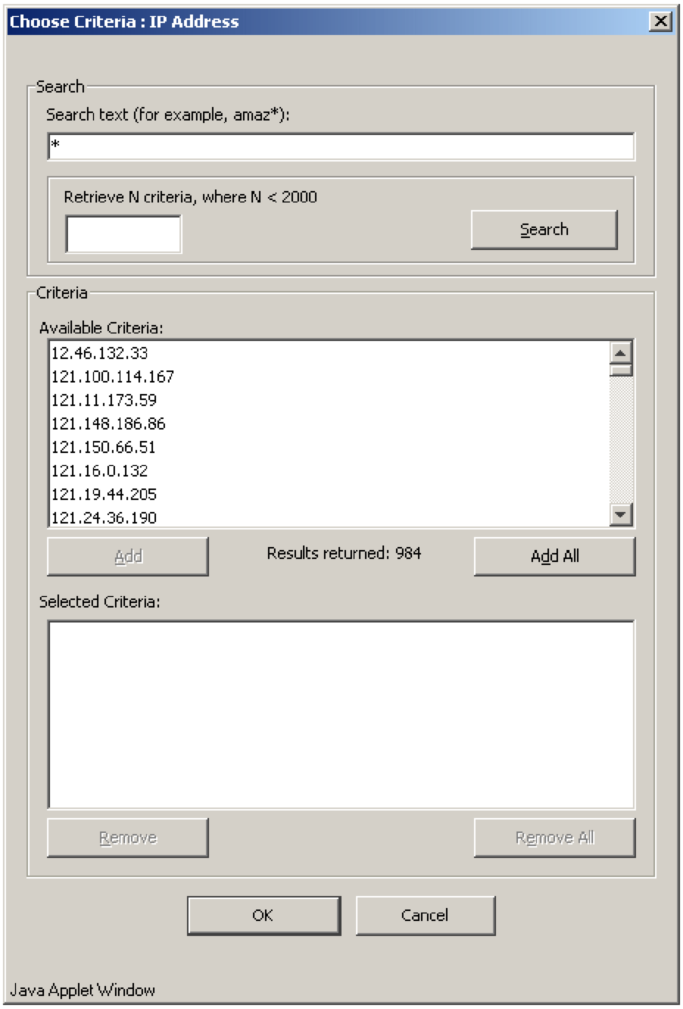
Use this tab to include or exclude IP addresses.

1. Select the **IP Address** tab.
2. To include all IP addresses in the report, select **Include all**.

3. To include or exclude specific IP addresses from the report, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add IP addresses.
   - If the Selected Criteria list contains IP addresses, the view does not change. Click **Add** to add IP addresses to the list, or click **Remove** to delete IP addresses.



4. Search for IP addresses.

   a. Enter search text.

      You can use wildcards.

   b. Enter the number of search requests to display (1 to 2000), and then click **Search**.

The search results are displayed in the **Available Criteria** list.

> **Note**
> To increase the maximum number of records returned to greater than 2000, consult the Knowledge Base at **www.websense.com/support** and search for "How to increase the maximum number of results when searching for items."

5. Select IP addresses from the **Available Criteria** list, and then click **Add**.
6. Click **Add All** to add all IP addresses from the availability list.

   The selected IP addresses are displayed in the **Selected Criteria** list.
7. To remove IP addresses from the **Selected Criteria** list, select the address, and then click **Remove**. To remove all IP addresses from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for IP addresses.

8. Click **OK**.

   The IP addresses are added to the **Selected Criteria** list in the **IP Address** tab.

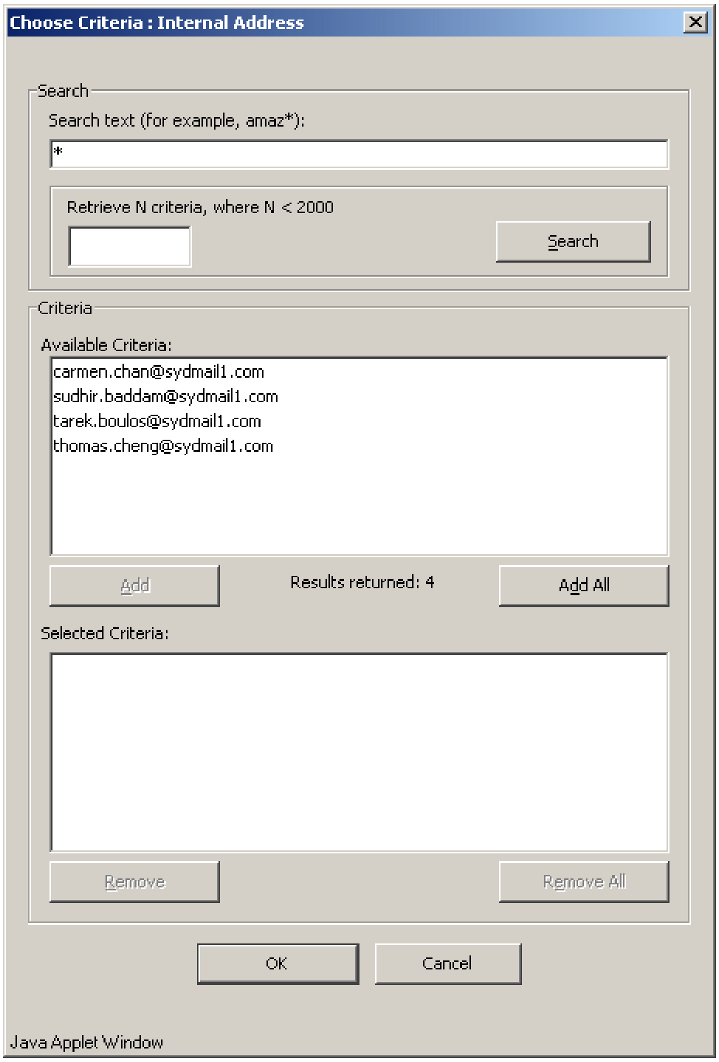
Internal Address

Use this tab to include or exclude internal email addresses.

1. Select the **Internal Address** tab.
2. To include all internal email addresses in the report, select **Include all**.
3. To include or exclude specific internal email addresses from the report, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add internal addresses.
   - If the Selected Criteria list contains internal addresses, the view does not change. Click **Add** to add internal addresses to the list, or click **Remove** to delete internal addresses.



4. Search for internal email addresses.
   a. Enter search text.

      You can use wildcards.
   b. Enter the number of search requests to display (1 to 2000), and then click **Search**.

      The search results are displayed in the **Available Criteria** list.

Note

To increase the maximum number of records returned to greater than 2000, consult the Knowledge Base at **www.websense.com/support** and search for “How to increase the maximum number of results when searching for items.”

5. Select internal email addresses from the **Available Criteria** list, and then click **Add**.
6. Click **Add All** to add all internal email addresses from the availability list.

   The chosen addresses are displayed in the **Selected Criteria** list.
7. To remove internal email addresses from the **Selected Criteria** list, select the addresses, and then click **Remove**. To remove all internal email addresses from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for internal addresses.

8. Click **OK**.

   The internal email addresses are added to the **Selected Criteria** list in the **Internal Address** tab.

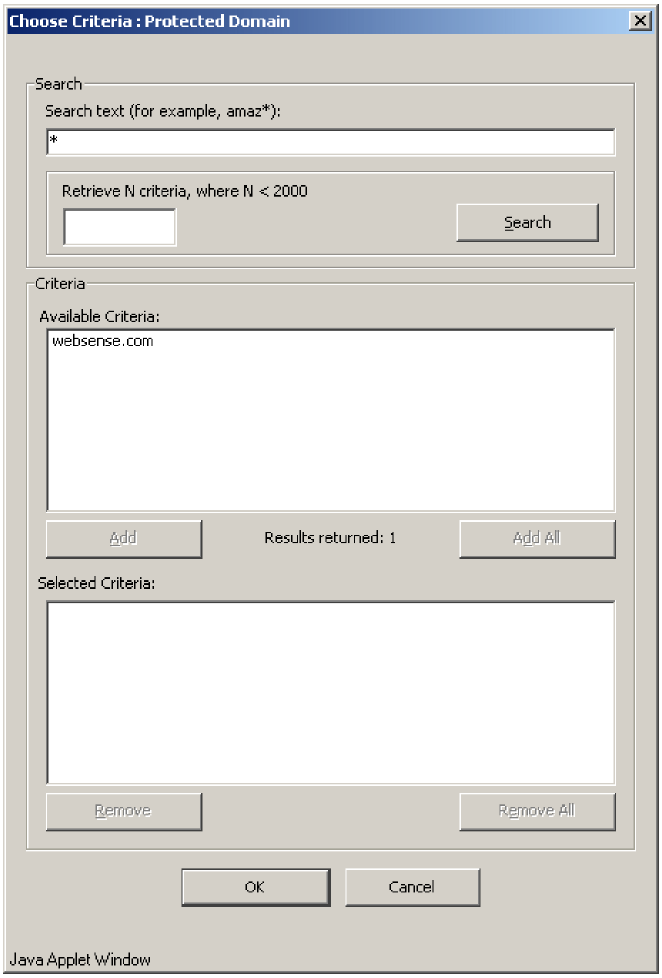
Protected Domain

Use this tab to include or exclude protected domains.

1. Select the **Protected Domain** tab.
2. To include all protected domains in the report, select **Include all**.
3. To include or exclude specific protected domains from the report, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add protected domains.
   - If the Selected Criteria list contains protected domains, the view does not change. Click **Add** to add protected domains to the list, or click **Remove** to delete protected domains.



4. Search for protected domains.
   a. Enter search text.

      You can use wildcards.
   b. Enter the number of search requests to display (1 to 2000), and then click **Search**.

      The search results are displayed in the **Available Criteria** list.

> **Note**
> To increase the maximum number of records returned to greater than 2000, consult the Knowledge Base at **www.websense.com/support** and search for “How to increase the maximum number of results when searching for items.”

5. Select protected domains from the **Available Criteria** list, and then click **Add**.
6. Click **Add All** to add all protected domains from the availability list.

   The chosen protected domains are displayed in the **Selected Criteria** list.

7. To remove protected domains from the **Selected Criteria** list, select the domains, and then click **Remove**. To remove all protected domains from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for protected domains.

8. Click **OK**.

   The protected domains are added to the **Selected Criteria** list in the **Protected Domain** tab.

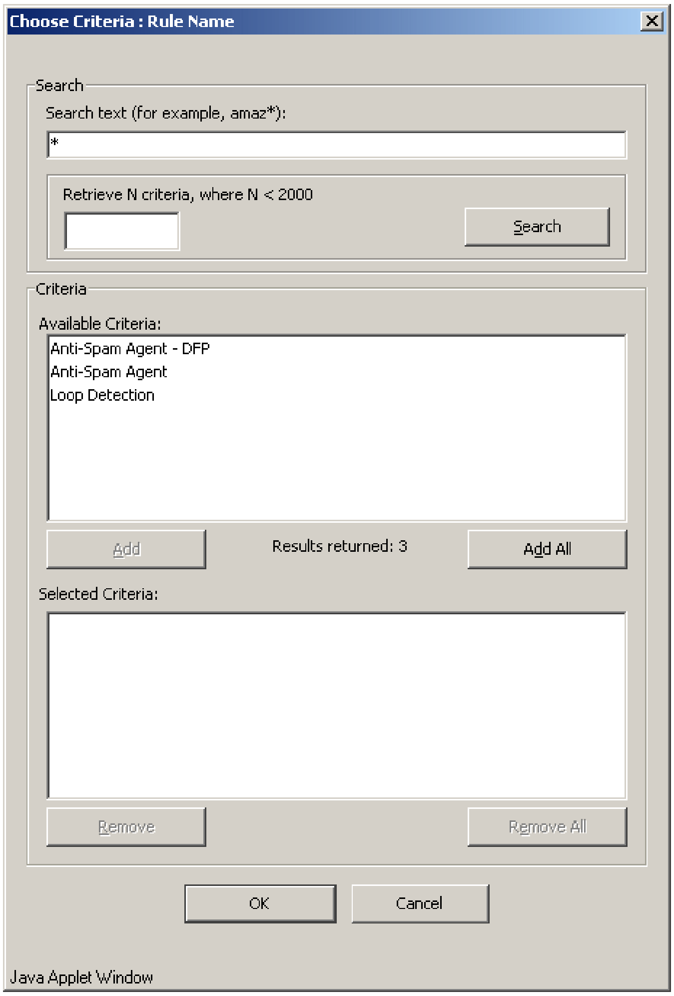
Rule Name

Use this tab to include or exclude rule names.

1. Select the **Rule Name** tab.
2. To include all rule names in the report, select **Include all**.
3. To include or exclude specific rule names from the report, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add rule names.
   - If the Selected Criteria list contains rule names, the view does not change. Click **Add** to add rule names to the list, or click **Remove** to delete rule names.



4. Search for rule names.
   a. Enter search text.

      You can use wildcards.

   b. Enter the number of search requests to display (1 to 2000), and then click **Search**.

      The search results are displayed in the **Available Criteria** list.

Note

To increase the maximum number of records returned to greater than 2000, consult the Knowledge Base at **www.websense.com/support** and search for “How to increase the maximum number of results when searching for items.”

5. Select rule names from the **Available Criteria** list, and then click **Add**.
6. Click **Add All** to add all rule names from the availability list.

   The selected rule names are displayed in the **Selected Criteria** list.

7. To remove rule names from the **Selected Criteria** list, select the names, and then click **Remove**. To remove all rule names from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for rule names.

8. Click **OK**.

   The rule names are added to the **Selected Criteria** list in the **Rule Names** tab.

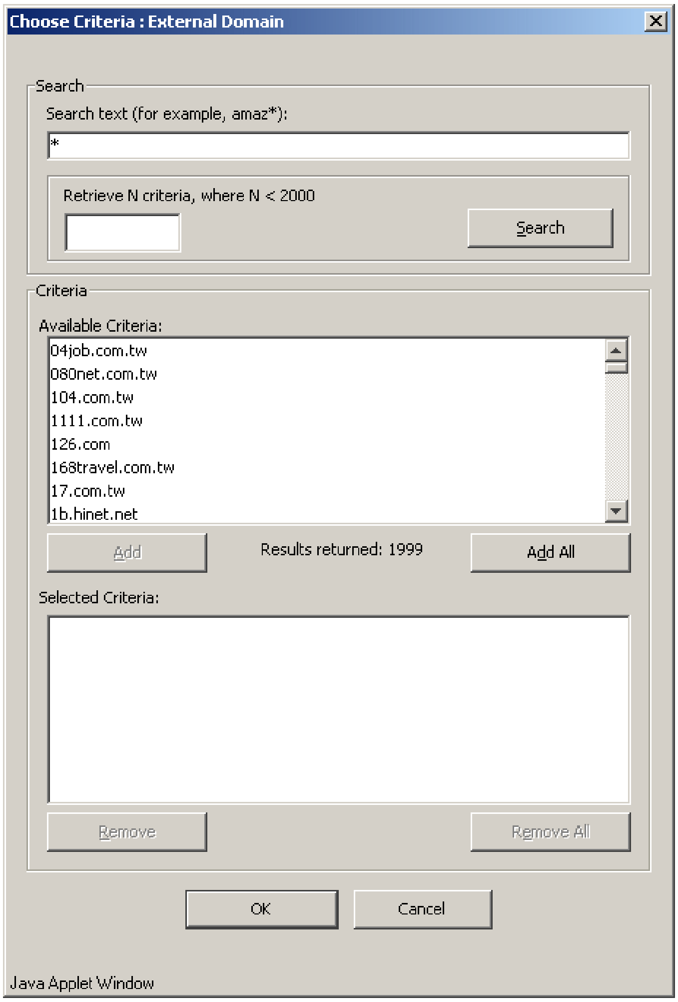
External Domain

Use this tab to include or exclude external domains.

1. Select the **External Domain** tab.
2. To include all external domains in the report, select **Include all**.
3. To include or exclude specific external domains, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add external domains.
   - If the Selected Criteria list contains external domains, the view does not change. Click **Add** to add domains to the list, or click **Remove** to delete external domains.



4. Search for external domains.
    a. Enter search text.

       You can use wildcards.
    b. Enter the number of search requests to display (1 to 2000), and then click **Search**.

       The search results are displayed in the **Available Criteria** list.

Note

To increase the maximum number of records returned to greater than 2000, consult the Knowledge Base at **www.websense.com/support** and search for “How to increase the maximum number of results when searching for items.”

5. Select external domains from the **Available Criteria** list, and then click **Add**.
6. Click **Add All** to add all external domains from the availability list.

The selected external domains are displayed in the **Selected Criteria** list.

7. To remove external domains from the **Selected Criteria** list, select the domains, and then click **Remove**. To remove all external domains from the list, click **Remove All**.

Note
Restricted users cannot change the criteria for external domains.

8. Click **OK**.

   The external domains are added to the **Selected Criteria** list in the **External Domain** tab.

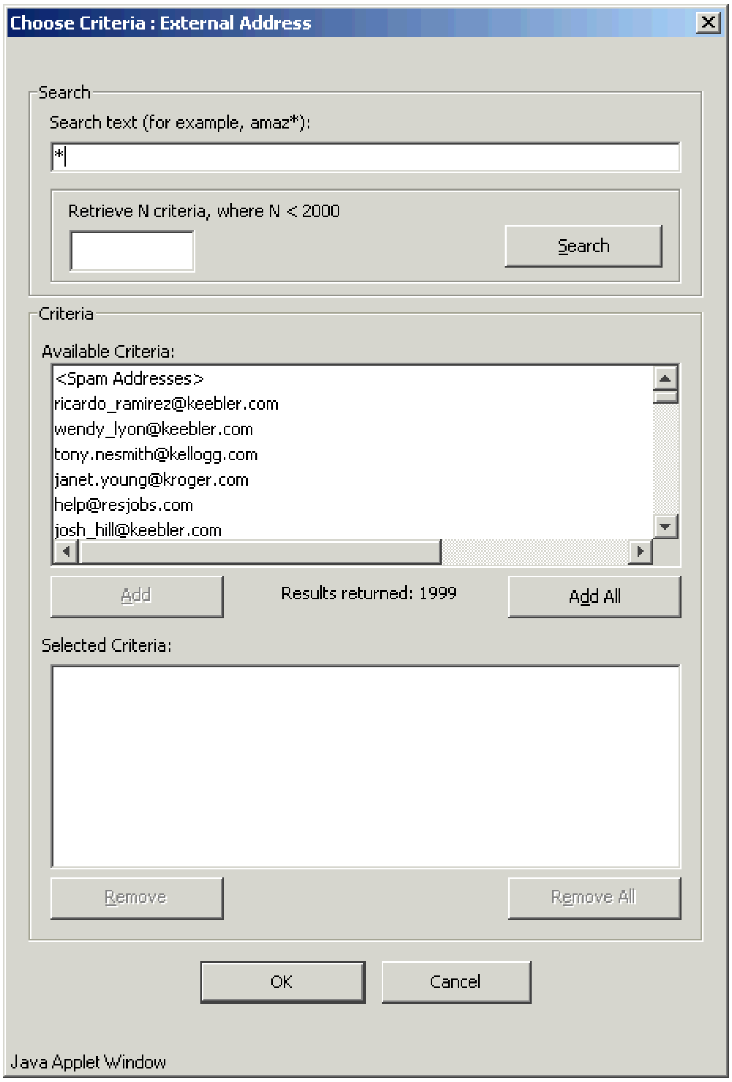
External Address

Use this tab to include or exclude external email addresses.

1. Select the **External Address** tab.
2. To include all external email addresses in the report, select **Include all**.
3. To include or exclude specific external email addresses, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add external email addresses.
   - If the Selected Criteria list contains external email addresses, the view does not change. Click **Add** to add external email addresses to the list, or click **Remove** to delete external email addresses.



4. Search for external email addresses.
    a. Enter search text.

       You can use wildcards.

    b. Enter the number of search requests to display (1 to 2000), and then click **Search**.

       The search results are displayed in the **Available Criteria** list.

Note

To increase the maximum number of records returned to greater than 2000, consult the Knowledge Base at **www.websense.com/support** and search for “How to increase the maximum number of results when searching for items.”

5. Select external email addresses from the **Available Criteria** list, and then click **Add**.
6. Click **Add All** to add all external email addresses from the availability list.

   The selected external email addresses are displayed in the **Selected Criteria** list.
7. To remove external email addresses from the **Selected Criteria** list, select the addresses, and then click **Remove**. To remove all email addresses from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for external addresses.

8. Click **OK**.

   The external email addresses are added to the **Selected Criteria** list in the **External Address** tab.

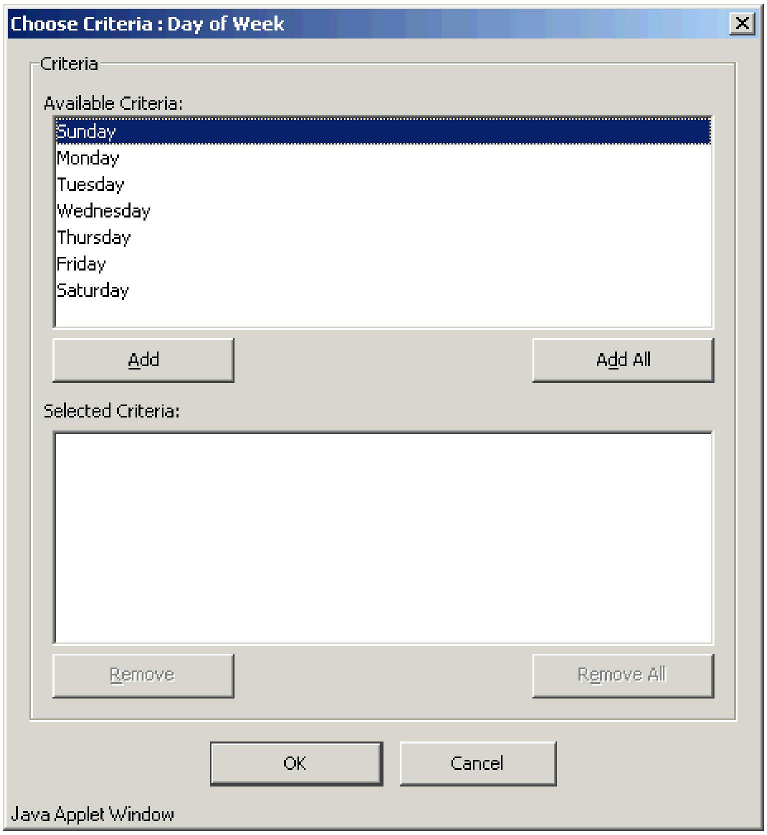
Day of Week

Use this tab to include or exclude the day that email messages have been sent or received.

1. Select the **Day of Week** tab.
2. To include all days of the week in the report, select **Include all**.
3. To include or exclude days of the week, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add days of the week.
   - If the Selected Criteria list contains days of the week, the view does not change. Click **Add** to add days of the week to the list, or click **Remove** to delete days of the week.



4. Select days from the **Available Criteria** list, and then click **Add**.
5. Click **Add All** to add all days of the week from the availability list.

   The selected days of the week are displayed in the **Selected Criteria** list.
6. To remove days from the **Selected Criteria** list, select the days, and then click **Remove**. To remove all days from the list, click **Remove All**.

Note
Restricted users cannot change the criteria for days of the week.

7. Click **OK**.

   The days are added to the **Selected Criteria** list in the **Day of Week** tab.

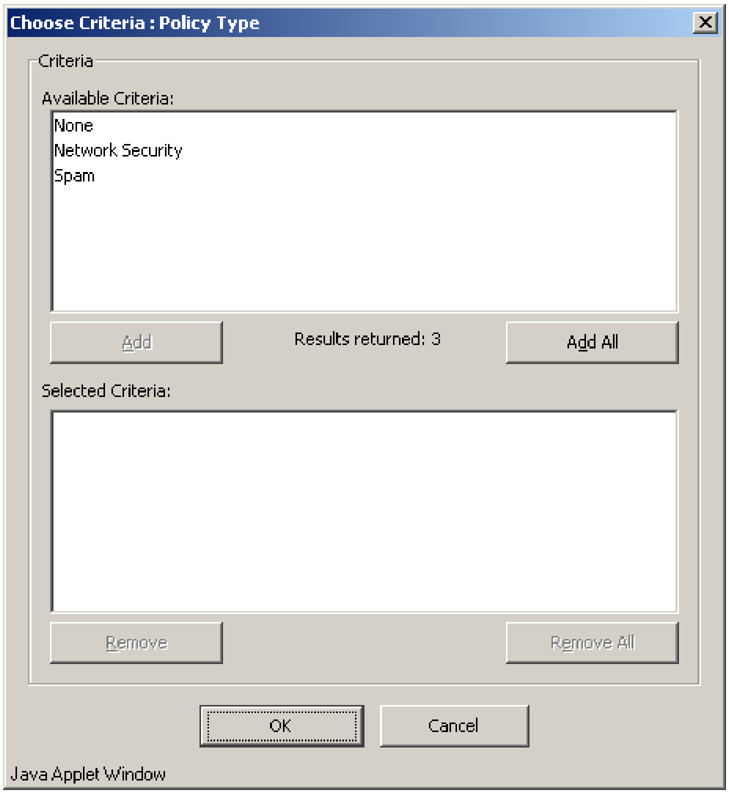
Policy Type

Use this tab to include or exclude policy types.

1. Select the **Policy Type** tab.
2. To include all policy types in the report, select **Include all**.
3. To include or exclude specific types, select either **Include selected items** or **Exclude selected items**.

One of the following actions occurs:

- If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add policy types.
- If the Selected Criteria list contains policy types, the view does not change. Click **Add** to add policy types to the list, or click **Remove** to delete policy types.



4. Select policy types from the **Available Criteria** list, and then click **Add**.
5. Click **Add All** to add all policy types from the availability list.

   The selected policy types are displayed in the **Selected Criteria** list.
6. To remove policy types from the **Selected Criteria** list, select the policy types, and then click **Remove**. To remove all policy types from the list, click **Remove All**.

Note
Restricted users cannot change the criteria for policy types.

7. Click **OK**.

   The policy types are added to the **Selected Criteria** list in the **Policy Type** tab.

Direction

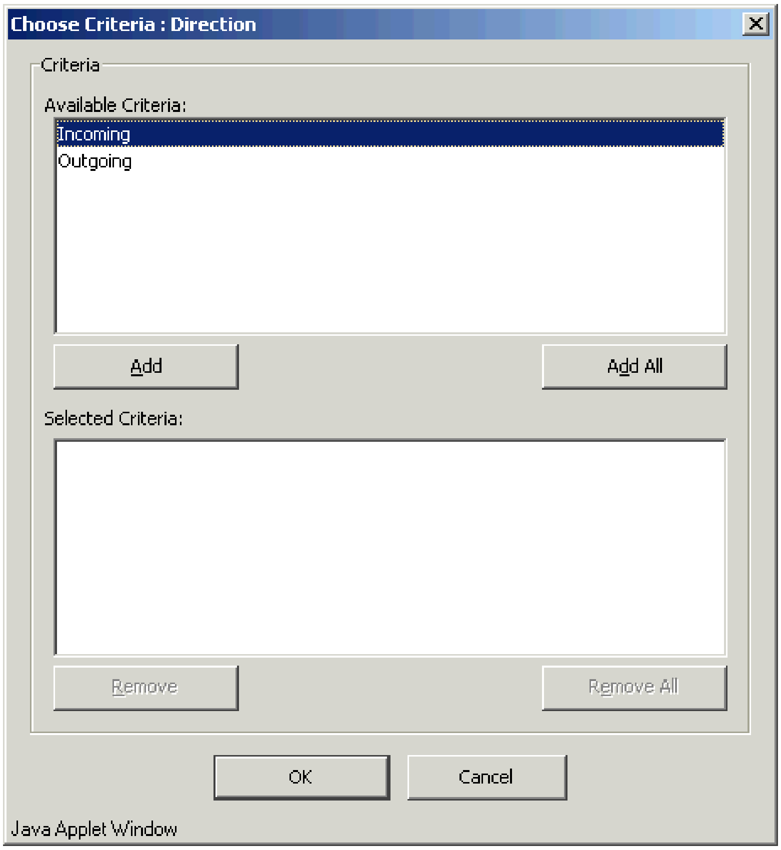
This tab is displayed for Forensic reports only. Use this tab to include or exclude the direction of email messages.

1. Select the **Direction** tab.
2. To include all inbound and outbound email messages in the report, select **Include all**.
3. To include or exclude either inbound, outbound or both directions, select either **Include selected items** or **Exclude selected items**.

   One of the following actions occurs:

   - If the Selected Criteria list is empty, the Choose Criteria dialog box appears automatically, allowing you to add direction types.
   - If the Selected Criteria list contains direction types, the view does not change. Click **Add** to add direction types to the list, or click **Remove** to delete direction types.

Note
If there are already directions in the **Selected Criteria** list on the **Direction** tab, click **Add** to display the Choose Criteria dialog box.



4. Select a direction from the **Available Criteria** list, and then click **Add**.
5. Click **Add All** to add both directions from the availability list.

   The selected directions are displayed in the **Selected Criteria** list.
6. To remove directions from the **Selected Criteria** list, select the direction, and then click **Remove**. To remove both directions from the list, click **Remove All**.

> **Note**
> Restricted users cannot change the criteria for directions.

7. Click **OK**.

   The directions are added to the **Selected Criteria** list in the **Direction** tab.

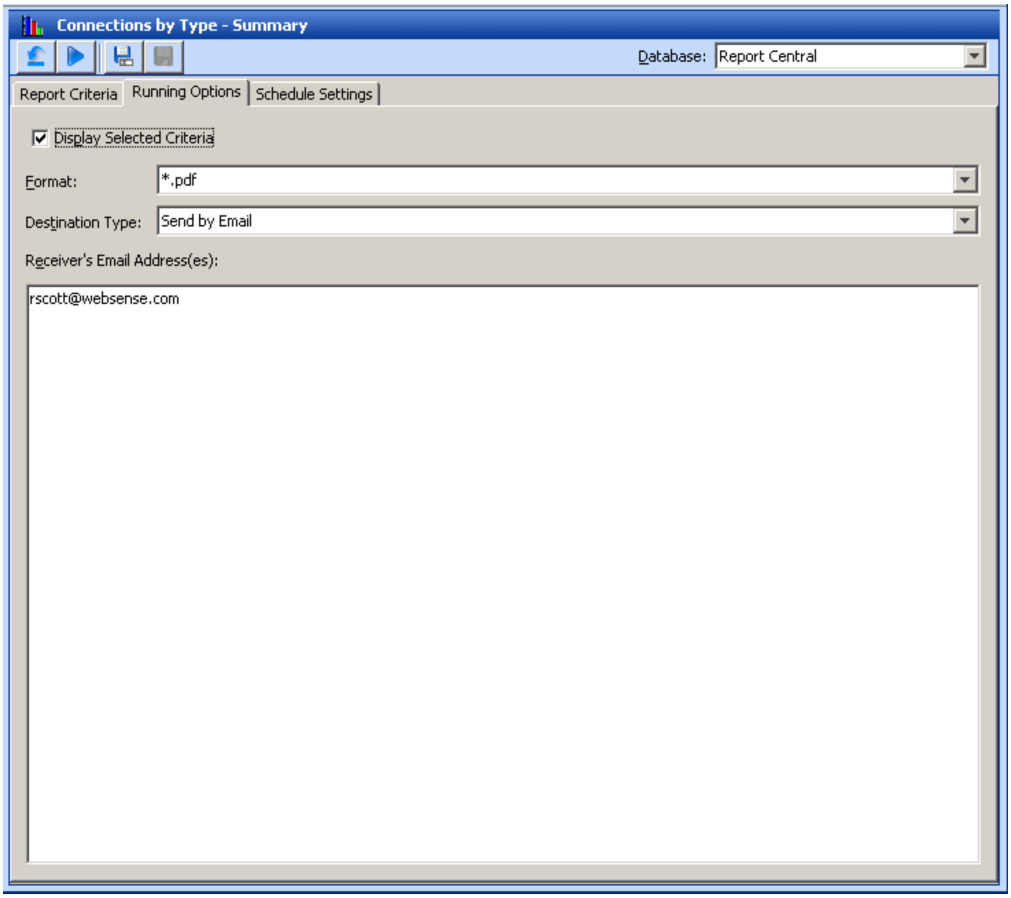
Options

The **Options** tab is available only for certain reports. The possible settings are:

- **Exclude Postmaster:** Not available for Trend or Management reports. Use this option to specify internal email addresses that are to be excluded from the report. For multiple email addresses, use a comma to separate the addresses.
- **Display Top N Results:** This option is used to specify a number of results, such as Top N IPs by Rule or Top N Rules Triggered. The default value for *N* is 15.
- **Virus cost:** This option is available only for the Return on Investment (ROI) report. This is the cost to your organization of each virus-carrying email that could enter your organization if you are not using Websense Email Security. The default value is $280.00.
- **Spam cost:** This option is available only for the Return on Investment (ROI) report. This is the cost to your organization of each spam email that could enter your organization if you are not using Websense Email Security. The default value is $0.04.

Running options

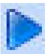
Use the **Running Options** tab to control how your report is produced and where it is saved.



To specify running options

1. Select the Running Options tab.
2. To display the report criteria, select **Display Selected Criteria**.
3. Select a report format from the list.
4. From the **Destination Type** menu, select how you want the report to be displayed.
5. If you have selected to send the report as an email, enter one or more email addresses in the **Receiver’s Email Address(es)** field.

> **Note**
> It is good practice to use PDF files as attachments to an email message.

6. Click **Run** to run the report. 

Display selected criteria

You can choose to display the report criteria on the last page. If you choose this option, the criteria that you selected are printed.

Note
If you use the default setting of including all criteria, the selected criteria are not shown, even if you select **Display Selected Criteria**.

Format

You can generate reports in the following formats:

Format	Details
.csv	Comma Separated Value: A text format that can be used by spreadsheet and database programs such as Microsoft Excel and Access
.htm	You can view the report in HTML format using a Web browser.
.pdf	Portable Document Format (PDF): Requires a reader, such as Adobe Acrobat Reader, to view. Adobe Acrobat Reader is available as a free download from www.adobe.com). **Note:** You need version 6 or later of Adobe Acrobat Reader to read reports in this format. **Note:** A good practice is to use PDF files as attachments to an email message.
.rtf	Rich Text Format: files can be viewed in word processors, such as Microsoft Word.
.xls	Microsoft Excel Format (version 8 or later)

Important

- For a secure (HTTPS) connection to Report Central, configure Internet Explorer to view reports in **pdf** and **rtf** format. Select **Tools** > **Internet Options**. Select the Advanced tab, and then clear the **Do not save encrypted pages to disk** check box.
- Pop-up blockers, such as those used by Google, Yahoo! or Microsoft Windows XP SP2, can prevent reports from displaying in your browser. Alter your settings to allow pop-ups from the Report Central address.

Destination type

You can specify how you want a report to display. Emailed reports are sent in their native, uncompressed format. If you are unsure about the size of a report to email, save the report to your machine using the **Schedule Settings** options. You can then check the size of the report before you send it. The following table shows the destination type options.

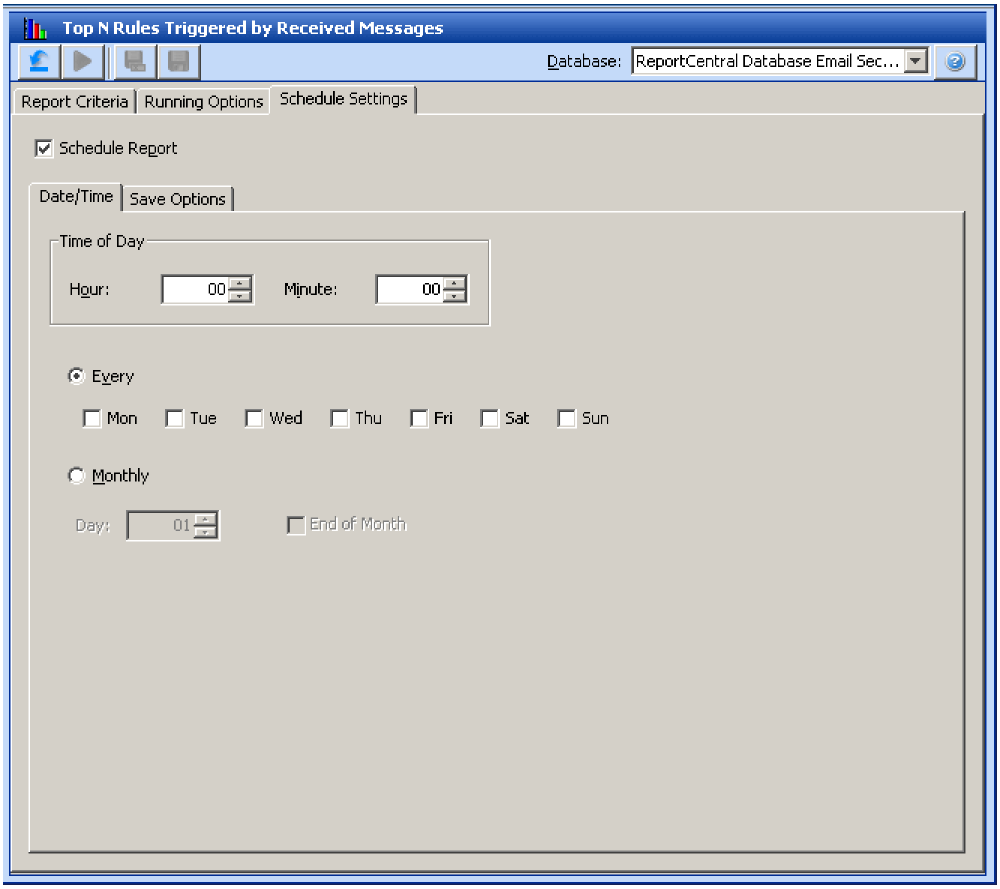
Option	Description
Show in Browser (default)	Reports in HTML and PDF format open automatically in a browser window.
Send by email	The report is sent as an attachment to the email address you specify. You can add multiple recipients by separating the addresses with a semicolon. **Note:** A good practice is to use PDF files as attachments to an email message.

Note

Some email programs may not preview HTML reports correctly; however, if you open the email, the report displays properly.

Schedule settings

Use the **Schedule Settings** tab to set up reports to run automatically at specific times or dates.



To enable report scheduling, select the **Schedule Report** check box. When you enable report scheduling, two tabs become available:

- Date/Time
- Save Options

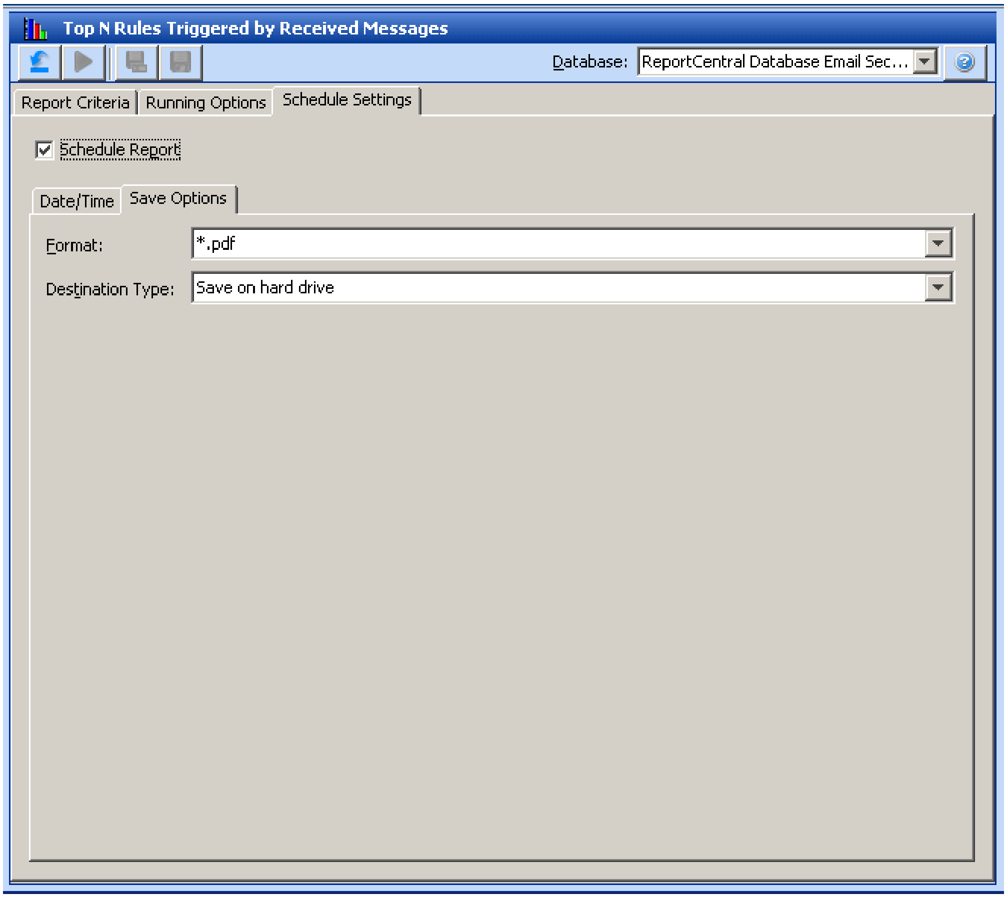
Date/Time

On this tab you can specify the following:

- **Time of Day**: Specify the hour and minute to run a report (using the 24-hour clock).
- **Every**: Specify on which days of the week to run reports. You can run reports every day, once a week, or on selected days.
- **Monthly**: Specify a day of the month to run a report, or run a report on the last day of the month. If you select the monthly check box, the Daily/Weekly options are unavailable.

Save Options

When the report you have scheduled is generated, you can save it to your hard drive automatically by specifying save options.



Option	Descriptions
Format	You can save the report in the following formats: • .csv • .htm • .pdf • .rtf • .xls See *Format*, page 81 for information about each format.
Destination type	**Save on hard drive**: The report is saved to your computer's hard drive. This is useful if you want to check the size of the file before sending it by email.
	Send by email: The report is sent as an attachment to the email address you specify. **Note:** It is good practice to use the PDF format for attachments.

Generating reports

When you have set up your criteria, you are ready to generate the report.

You can:

- Save the settings to a different report name. 
- Save to replace the default settings (available only for saved reports). 
- Generate the report. 

Use the **Database** drop-down list box to select the database from which to run your reports.

For details about the save options, see *Saving reports*, page 85. If you do not select a save option, your settings are discarded when you log out of Report Central.

Managing large reports

Forensic reports can generate extremely large volumes of data, especially in large organizations with heavy network traffic. Report Central limits the amount of information to 20,000 lines (approximately 1000 pages) for each report. If you run reports that exceed this limit, a note is added to the first page of the report.

There are two ways to manage large reports:

- Print the report to file. You can view the report without having to print it, or print only selected pages. See *Save Options*, page 84 for details.
- Constrain a scheduled report by limiting the range of data in specific criteria, such as Internal Address or IP Address.

Saving reports

When you have set up your report, you can save a copy to your hard drive. There are two places to save a report:

- Shared folder
- Personal folder

See *User accounts*, page 15 for information about defining permissions for accessing a folder.

Shared and Personal folders

Any user can view report criteria saved in the Shared folder. Users with the necessary permissions can also change the report criteria. A report saved in a Personal folder can be viewed only by the user who created it.

> **Note**
> If you change a report in the Shared folder, select **Save As** to make sure that you do not overwrite another user's report.

To save a report to a Shared or Personal folder:

1. Set up the report using your required criteria and options.
2. Click **Save As**.

   The **Save Report** dialog box opens.
3. Select the folder in which to save the report.
4. In the **Report Name** field, enter a name for your report.
5. Click **Save**.

   The **Report History** tab is displayed in the dialog box. See *Report history*, page 59 for details.

This tab displays a list of the reports that have been run according to your schedule. For details about scheduling reports, see *Schedule settings*, page 83.

Displaying saved reports

When you save a report to a Shared or Personal folder, the Report History tab appears in Report Manager. This tab shows the scheduled reports that have been generated.

> **Note**
> Only reports that have been saved using the **Save on hard drive** option are displayed in the Report History tab (see *Save Options*, page 84). Reports sent by email are not displayed.

Managing shared and personal folders

- To create folders within the Shared and Personal folders, select the folder, and then click .
- To delete reports or folders from Shared and Personal folders, select the item, and then click .

Index

R

S