

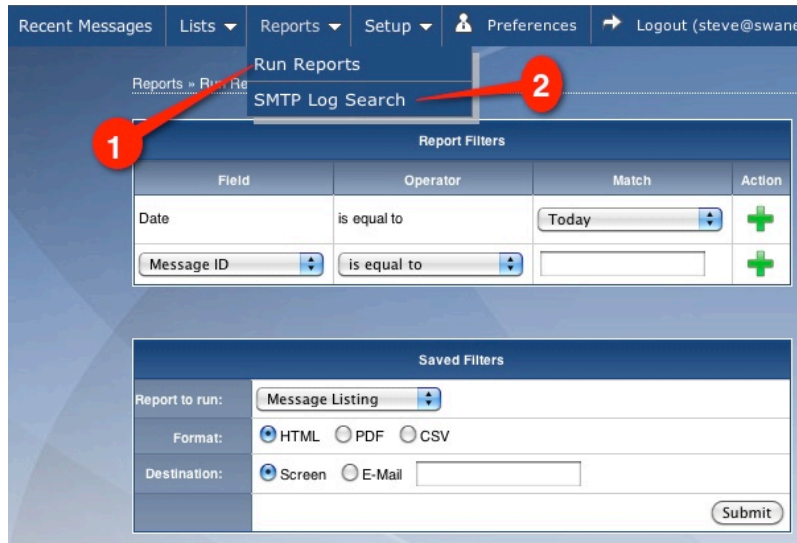


reporting for barricademx plus systems
documentation for system and domain administrators

Reporting for BarricadeMX Plus

Reporting functions are only available to users who are logged in as System Administrators or Domain Administrators. These monitoring functions can be found by accessing the Top Level **Reports** pull-down menu:

Accessing the Reporting Functions



The screenshot shows the top navigation bar with the following items: Recent Messages, Lists, Reports, Setup, Preferences, and Logout (steve@swane). The Reports menu is open, showing two options: Run Reports (marked with a red circle and the number 1) and SMTP Log Search (marked with a red circle and the number 2). Below the menu is the 'Report Filters' section, which contains a table with columns for Field, Operator, Match, and Action. The table has two rows: one for 'Date' with the operator 'is equal to' and a 'Today' dropdown, and another for 'Message ID' with the operator 'is equal to' and an empty dropdown. Below the table is the 'Saved Filters' section, which includes a 'Report to run:' dropdown set to 'Message Listing', a 'Format:' section with radio buttons for HTML (selected), PDF, and CSV, and a 'Destination:' section with radio buttons for Screen (selected) and E-Mail, followed by an empty text input field and a 'Submit' button.

Figure 1, Top Menu

Selecting **1. Run Reports** will allow you to report on messages that have successfully passed through BarricadeMX filtering

Selecting **2. SMTP Log Search** will allow you to report on all smtpf connections that have been seen by the smtpf process.

Run Reports Data Log Search Data

All connections, messages that are rejected and returned to the sender and messages that are accepted for further filtering are stored in the **bmlog** table in the Postgres database. Because of the large amount of data in this table, (every MTA connection from all email gateways) data in this table is only stored for three days.

Important: If a message is rejected by the BarricadeMX (the smtpf application) screening process, it will not be displayed in the **Recent Messages** screens and no data for the message will be available to the **Reports -> Run Reports** functions.

Data on messages that have been rejected by BarricadeMX screening will only be available by using the **Reports -> SMTPF Log Search** function and this data is only kept for three days.

Run Reports Data

Details for messages that pass BarricadeMX screening are logged to the Postgres Database in the **maillog** table. This is the same data that is seen on the **Recent Messages** screens. Typically, this detailed message data is stored for 30 days.

Important: If a message is rejected by the BarricadeMX (smtpf process) screening process, it will not be displayed in the Recent Messages screens and no data for the message will be available to the **Reports -> Run Reports** functions.

Data on messages rejected by BarricadeMX screening will only be available by using the **Reports -> SMTPF Log Search** function and this data is only kept for three days.

Using the SMTPF Log Search function

Selecting **SMTP Log Search** from the top-level menu will bring up the Log Search data entry screen.



Figure 2, Top, Recent Messages Screen

As the screen explains, any of the following items may be entered in the In the **Search** text box:

- IP Address
- CIDR Mask
- Senders e-mail address
- Senders e-mail domain
- SMTP Session ID

then select the **2**. Search “Arrow” to display the search results as shown below;

Reports » SMTP Log Search

This utility allows you to search the raw SMTP logs from the last 3 days.

You may search by any of the following:
 IP address
 CIDR Mask
 Senders e-mail address
 Senders e-mail domain
 SMTP Session ID

Search: >

Date/Time	Session #	IP	PTR	HELO	Transaction Count	Message Count
03/13/2011 11:13:55 AM	n2CBDp051334352600	99.151.240.108	mail.careplusfinancia.com	mailer.careplusfinancia.com	1	0

Transaction #	Recipients	Sender	Recipient	Status
n2CBDr0513343526Cy	0	ext_1@emm.careplusfinancia.com	sotto@shadeamerica.com	250 2.1.5 recipient accepted #297 (n2CBDp051334352600)

Last Session Error: 451 4.7.0 try again later #552 (n2CBDp051334352600)* p0f="(unknown) hops 0

Figure 3, Bottom Recent Messages Screen

If any matching records are found, the:

- Date/Time
- Session ID
- IP address
- DNS PTR record of the sending server
- “HELO” record sent by the sending server
- Transaction Count
- Message Count
- Transaction ID
- Number of recipients
- Sender
- Recipient
- Status
- Last Session Error

Will be displayed for each record found in the Postgres **bmxmlg** table. In the event that more data is required, you can use the Session ID or the Transaction ID to manually search the maillog text logs that can be found in /var/log/maillog. Please see [How To Use grep Command In Linux / UNIX for instructions on how to search a text file for a specific text string.](#)

Using the SMTPF Log Search function

Selecting **Run Reports** from the top-level menu will bring up the MailWatch Reports data entry screen

The screenshot shows the MailWatch Reports data entry screen. The top navigation bar includes 'Recent Messages', 'Lists', 'Reports', 'Setup', 'Preferences', and 'Logout (steve@swaney.com)'. The main content area is divided into three sections:

- Report Filters:** A table with columns 'Field', 'Operator', 'Match', and 'Action'. A filter is added with 'Message ID' as the field, 'is equal to' as the operator, and an empty match field. A green plus sign is in the action column.
- Active filters:** A table with columns 'Field', 'Operator', 'Match', and 'Action'. It contains two filters: 'Date (YYYY-MM-DD)' with 'is equal to' operator and 'Last 7 Days' match, and 'From Domain' with 'is equal to' operator and 'cnet.online.com' match. Both have a red 'X' in the action column.
- Saved Filters:** A form with fields for 'Save filter:' (containing '7_day_cnet'), 'Report to run:' (a dropdown menu with 'Message Listing' selected), 'Format:' (radio buttons for HTML, PDF, CSV), and 'Destination:' (radio buttons for Screen, E-Mail). A 'Submit' button is at the bottom right.

Numbered callouts (1-13) point to various elements: 1 (Field), 2 (Operator), 3 (Match), 4 (Add symbol), 5 (Active filters table), 6 (Filter in Active filters), 7 (Save filter text box), 8 (Report to run dropdown), 9 (Destination radio buttons), 10 (Submit button), 11 (Save filter button), 12 (Save filter button), and 13 (Submit button).

Figure 4, Top, Message Detail Screen

To add a filter select the **1. Field**, **2. Operator** and fill in the **3.** text field with the expression to **Match**, then select the **4.** Add symbol.

The Filter you have added will then show up in the **Active filters** list. In the example above we have added a filter. Filter **6.** In the example above adds a filter that will find any messages where the from domain matches “cnet.online.com”

You should then select the:

- **7.** Report to run **Format**. Message listing is the most commonly used format but many other are available.
- **8.** Report format. **HTML** is the default but **PDF** and **CSV** formats are available.
- **9.** Destination. **Screen** or **E-mail** formats are available. If you **select E-mail**, you must fill in a valid email address in the text box and **ONLY** CVS or PDF formats are available if **E-mail** is selected.

You may save your search criteria for re-loading later. Simply give the report a name in the text box next to **11. Save filter** and then select **12. Save**.

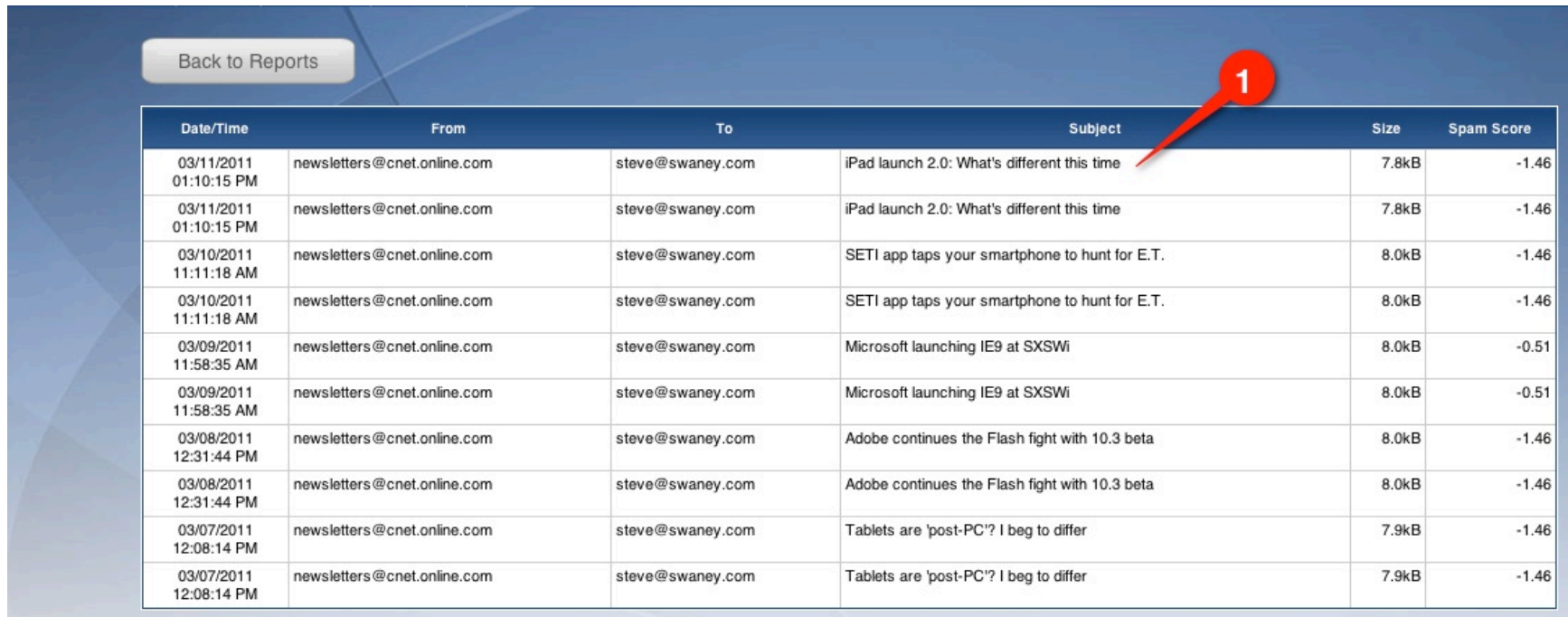
When you have completed filling in the form, select **13. Submit** to run and display or send the Report.

Using the Report

If you selected the default setting of:

- **Report to run:** Message Listing
- **Format:** HTML
- **Destination:** Screen

You should see a screen similar to the one below.



The screenshot shows a web interface with a 'Back to Reports' button and a table of message listings. A red callout bubble with the number '1' points to the 'Subject' column header.

Date/Time	From	To	Subject	Size	Spam Score
03/11/2011 01:10:15 PM	newsletters@cnet.online.com	steve@swaney.com	iPad launch 2.0: What's different this time	7.8kB	-1.46
03/11/2011 01:10:15 PM	newsletters@cnet.online.com	steve@swaney.com	iPad launch 2.0: What's different this time	7.8kB	-1.46
03/10/2011 11:11:18 AM	newsletters@cnet.online.com	steve@swaney.com	SETI app taps your smartphone to hunt for E.T.	8.0kB	-1.46
03/10/2011 11:11:18 AM	newsletters@cnet.online.com	steve@swaney.com	SETI app taps your smartphone to hunt for E.T.	8.0kB	-1.46
03/09/2011 11:58:35 AM	newsletters@cnet.online.com	steve@swaney.com	Microsoft launching IE9 at SXSWi	8.0kB	-0.51
03/09/2011 11:58:35 AM	newsletters@cnet.online.com	steve@swaney.com	Microsoft launching IE9 at SXSWi	8.0kB	-0.51
03/08/2011 12:31:44 PM	newsletters@cnet.online.com	steve@swaney.com	Adobe continues the Flash fight with 10.3 beta	8.0kB	-1.46
03/08/2011 12:31:44 PM	newsletters@cnet.online.com	steve@swaney.com	Adobe continues the Flash fight with 10.3 beta	8.0kB	-1.46
03/07/2011 12:08:14 PM	newsletters@cnet.online.com	steve@swaney.com	Tablets are 'post-PC'? I beg to differ	7.9kB	-1.46
03/07/2011 12:08:14 PM	newsletters@cnet.online.com	steve@swaney.com	Tablets are 'post-PC'? I beg to differ	7.9kB	-1.46

Figure 4, Top, Message Detail Screen

Double click on any message line to display the **Message Details** screen. Please see the **monitoring barricademx plus systems** Section of the BarricadeMX documentation for more information on the **Message Details** screen.

Logout

To finish using the Web interface and return to the login screen, simply select the Logout tab at the left of the Top Menu on the screen.

Additional Support

For additional support please contact the support desk at your Company, your Internet Service Provider or Email Services Provider.