

**IronPort AsyncOS™ 5.0**  
**REPORTING API**  
for IronPort Appliances



---

## **COPYRIGHT**

Copyright © 2006 by IronPort Systems™, Inc. All rights reserved.

Revision Date: December 22, 2006

The IronPort logo, IronPort Systems, Messaging Gateway, Virtual Gateway, SenderBase, Mail Flow Monitor, Virus Outbreak Filters, Context Adaptive Scanning Engine (CASE), IronPort Anti-Spam, and AsyncOS are all trademarks or registered trademarks of IronPort Systems, Inc. Brightmail, the Brightmail logo, BLOC, BrightSig, and Probe Network are trademarks or registered trademarks of Symantec Incorporated. All other trademarks, service marks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.

This publication and the information contained herein is furnished "AS IS" and is subject to change without notice.

Publication of this document should not be construed as a commitment by IronPort Systems, Inc. IronPort Systems, Inc., assumes no responsibility or liability for any errors or inaccuracies, makes no warranty of any kind with respect to this publication, and expressly disclaims any and all warranties of merchantability, fitness for particular purposes and non-infringement of third-party rights.

Some software included within IronPort AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in IronPort license agreement.

The full text of these agreements can be found here:

[https://support.ironport.com/3rdparty/AsyncOS\\_User\\_Guide-1-1.html](https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html). Portions of the software within IronPort AsyncOS is based upon the RRdtool with the express written consent of Tobi Oetiker. Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of Symantec Incorporated. Portions of this document are reproduced with permission of Sophos Plc. Portions of this document are reproduced with permission of Brightmail Incorporated.

Brightmail Anti-Spam is protected under U.S. Patent No. 6,052,709.



## **IRONPORT SYSTEMS®, INC. CONTACTING IRONPORT CUSTOMER SUPPORT**

IronPort Systems, Inc.  
950 Elm Ave.  
San Bruno, CA 94066

If you have purchased support directly from IronPort Systems, you can request our support by phone, email or online 24 hours a day, 7 days a week. During our office hours (24 hours per day, Monday through Friday excluding US holidays), one of our engineers will contact you within an hour of your request. To report a critical issue that requires urgent assistance outside of our office hours, please call us immediately at the numbers below.

U.S. Toll-free: 1 (877) 641-IRON (4766)

International: [www.ironport.com/support/contact\\_support.html](http://www.ironport.com/support/contact_support.html)

Support Portal: [www.ironport.com/support](http://www.ironport.com/support)

If you have purchased support through a reseller or another entity, please contact them for support of your IronPort products.

---

---

# Table of Contents

<b>1. Reporting API</b> .....	<b>1</b>
Reporting API Overview .....	2
Downloading Reporting Data .....	2
Retrieving CSV Data via Automated Processes .....	2
Reporting Glossary .....	4
Reporting Data Descriptions .....	5
Table Keys .....	5
Common Entries .....	5
Incoming and Outgoing Mail Summary .....	5
Incoming Mail Details .....	6
Sender Group Details .....	9
Internal Users .....	10
Content Filters .....	12
Virus Outbreak Filters .....	14



---

# Reporting API

This document provides an overview of the IronPort appliance's Reporting API feature, the information necessary to retrieve reporting data, and a description of the data available through the API.

This chapter contains the following contents:

- “Reporting API Overview” on page 2
- “Downloading Reporting Data” on page 2
- “Reporting Glossary” on page 4
- “Reporting Data Descriptions” on page 5

## REPORTING API OVERVIEW

The Reporting API feature allows you to download the same data collected by the Email Security Monitor component of the IronPort appliance in a comma separated value (CSV) format. This format allows users to integrate the IronPort appliance's data gathering capabilities into other IT and business reporting systems.

## DOWNLOADING REPORTING DATA

You can retrieve the data used to build the charts and graphs in the Email Security Monitor feature via HTTP. This is useful if you plan to perform further analysis on the data via other tools. The data is available in standard comma separated value (CSV) format. The easiest way to get the HTTP query you will need is to configure one of the Email Security Monitor pages to display the type of data you want. You can then simply click the Export... link to initiate the download process.

### Retrieving CSV Data via Automated Processes

You can automate the retrieval of data from Email Security Monitor, for example, by an automatic script that will download raw data, process, and then display the results in some other system.

The easiest way to get the HTTP query you will need is to configure one of the Email Security Monitor pages to display the type of data you want. You can then copy the Export... link. This is the download URL. When automating data retrieval like this it is important to note which parameters in the download URL should be fixed and which should change (see below).

The download URL is encoded in such a way that it can be copied to an external script that can execute the same query (using proper HTTP authentication) and get a similar data set. The script can use Basic HTTP Authentication or cookie authentication. Keep the following in mind when retrieving CSV data via automated processes:

- Time range selection (past hour, day, week, etc.) in relation to when the URL is used again. If you copy the URL to retrieve a CSV data set for "Past Day," the next time you use that URL you will get a new data set that covers the "Past Day" from the time you send the URL again. The date range selection is retained, and appears in the CSV query string (e.g. `date_range=current_day`).
- Filtering and grouping preferences for the data set. Filters are retained and appear in the query string. Note that filters in reports are rare - one example is the "Global / Local" outbreaks selector in the Virus Outbreaks report.
- The CSV download returns all rows of data in the table for the selected time range.
- The CSV download returns the rows of data in the table ordered by timestamp and key. You can perform further sorting in a separate step such as via a spreadsheet application.
- The first row contains column headers that match the display names shown in the report. Note that timestamps (see "Timestamps" on page 3) and keys (see "Keys" on page 3) also appear.

### Sample URL Using the 'Export' Link

```
http://example.com/monitor/  
content_filters?format=csv&sort_col_ss_0_0_0=MAIL_CONTENT_FILTER_INCOM  
ING.RECIPIENTS_MATCHED&section=ss_0_0_0&date_range=current_day&sort_or  
der_ss_0_0_0=desc&report_def_id=mga_content_filters
```

**Note** — Some of the URL parameters in the above example are not essential for a CSV download. For example, you can use the following simplified URL to download the same data: `http://example.com/monitor/content_filters?format=csv&section=ss_0_0_0&date_range=current_day&report_def_id=mga_content_filters`

### Adding Basic HTTP Authentication credentials

To specify basic HTTP Authentication credentials to the URL:

```
http://example.com/monitor/
```

becomes:

```
http://username:password@example.com/monitor/
```

### File Format

The downloaded file is in CSV format and has a .csv file extension. The file header has a default filename, which starts with the name of the report, then the section of the report.

### Timestamps

Exports that stream data show begin and end timestamps for each raw “interval” of time. Two begin and two end timestamps are provided - one in numeric format and the other in human readable string format. The timestamps are in GMT time, which should make log aggregation easier if you have servers in multiple time zones.

Note that in some rare cases where the data has been merged with data from other sources, the export file does not include timestamps. For example, the Virus Outbreak Details export merges report data with Threat Operations Center (TOC) data, making timestamps irrelevant because there are no intervals.

### Keys

Exports also include the report table key(s), even in cases where the keys are not visible in the report. In cases where a key is shown, the display name shown in the report is used as the column header. Otherwise, a column header such as “key0,” “key1,” etc. is shown.

### Streaming

Most exports stream their data back to the client because the amount of data is potentially very large. However, some exports return the entire result set rather than streaming data. This is typically the case when report data is aggregated with non report data (e.g. Virus Outbreaks Detail.)

## REPORTING GLOSSARY

This section defines some commonly used terms and phrases in the Email Security Monitor reporting pages. Please refer to the product documentation for more details.

### Messages

Email Security Monitor reports on “messages” based on the number of recipients per email. For example, an incoming message from example.com sent to three recipients would count as three messages coming from that sender.

### Domains

Email Security Monitor rolls up statistics for IP addresses and hostnames to entities called domains, which are determined by a list of top level domains (TLD) and second level domains (SLD) provided by IronPort. For example, reporting data for mx1.ironport.com and mx2.ironport.com will be reported under ironport.com because “com” is a TLD. Some domains such as co.uk and fed.us are handled as special cases because these SLDs contain large networks. In such cases, IronPort will report on the domain that is one level lower in the hostname. Most exports stream their data back to the client because the amount of data is potentially very large. Please contact IronPort Customer Support if you need to add custom second level domains to your IronPort appliances.

### Outgoing Mail

Email Security Monitor counts a message as “outgoing” if it matches and is processed under a RELAY policy.

### Internal User

For incoming mail, Internal Users are the users for which your IronPort appliance received email, based on the Rcpt To: address. For outgoing mail, Internal Users are based on the Mail From: address and are useful when tracking the types of email that senders on your internal network are sending.

### Reputation Filtering ‘Multiplier’

Because messages blocked by reputation filtering do not actually enter the work queue, the appliance does not have access to the list of recipients for an incoming message. In this case, a multiplier is used to estimate the number of recipients. This multiplier was determined by IronPort Systems, Inc. and based upon research of a large sampling of existing customer data. Please contact IronPort Customer Support if you need to change the value of this multiplier.



## REPORTING DATA DESCRIPTIONS

The tables that follow describe the columns included in each of the .csv files available for download. The GUI page containing the export link to retrieve the .csv file is listed with each report below.

### Table Keys

The keys for a table (if any) are identified using an asterisk (\*).

### Common Entries

The first four columns for all the tables are identical. These columns are described below

Table 1-1 Common Table Columns

Parameter Name	Description
Begin Timestamp	Seconds since the Unix Epoch at the beginning of the measurement interval.
End Timestamp	Seconds since the Unix Epoch at the end of the measurement interval.
Begin Date	The human readable time stamp at the beginning of the measurement interval.
End Date	The human readable time stamp at the end of the measurement interval.

## Incoming and Outgoing Mail Summary

### Incoming Mail Summary

GUI Page containing 'Export' link: 'Overview'

Parameter Name	Description
Stopped by Reputation Filtering	Messages stopped by Reputation Filtering. This is calculated as: (Connections blocked by SBRS and HAT policies) * Multiplier + Recipients blocked by recipient throttling
Stopped as Invalid Recipients	Number of recipients rejected due to invalid recipients identified by conversational LDAP acceptance or RAT restrictions.
Spam Detected	Number of messages (recipients) identified as spam or suspect spam
Virus Detected	Number of messages (recipients) identified as virus positive
Stopped by Content Filters	Number of messages (recipients) that triggered at least one content filter with an action of drop, bounce, or quarantine

Parameter Name	Description
Clean messages	Total clean messages (recipients)

**Outgoing Mail Summary**

GUI Page containing 'Export' link: 'Overview'

Parameter Name	Description
Virus Detected	Total messages (recipients) identified as virus positive
Stopped by Content Filters	Total messages (recipients) that triggered at least one content filter with an action of drop, bounce, or quarantine
Clean Messages	Total clean messages (recipients)

**Outgoing Mail Delivery Details**

GUI Page containing 'Export' link: 'Overview'

Parameter Name	Description
Hard Bounces	Number of hard bounced messages (recipients)
Delivered	Number of outgoing messages delivered
Total Messages Delivered	Total outgoing messages (recipients) delivered

**Incoming Mail Details**

**Incoming Domains**

GUI Page containing 'Export' link: 'Incoming Mail: Domains'

Parameter Name	Description
Domain (*)	Name of the domain
Total Attempted	Total attempted messages (recipients) for this domain
Stopped by Recipient Throttling	Number of recipient messages stopped as a result of HAT limits

Parameter Name	Description
Stopped by Reputation Filtering	Messages stopped by Reputation Filtering from this domain. Includes the number of recipients stopped by recipient throttling
Stopped as Invalid Recipients	Number of recipients rejected from this domain due to invalid recipients identified by conversational LDAP acceptance or RAT restrictions.
Spam Detected	Number of messages (recipients) from this domain identified as spam or suspect spam
Virus Detected	Number of messages (recipients) from this domain identified as virus positive
Stopped by Content Filter	Number of messages (recipients) from this domain that triggered at least one content filter with an action of drop, bounce, or quarantine
Connections Rejected	Total connections rejected from this domain
Connections Accepted	Total connections accepted from this domain
Total Threat	Total threat messages from this domain
Clean	Total clean messages from this domain

### Incoming IP Addresses

GUI Page containing 'Export' link: 'Incoming Mail: IP Addresses'

Parameter Name	Description
IP Address (*)	IP Address
Hostname	Full hostname corresponding to this IP address
DNS Verified	Whether or not a reverse DNS lookup on the IP address matched the hostname provided by the remote host.
SBRS	Last Senderbase Reputation Score for this IP address during the time period being reported. Note that the SBRS for an IP address can change over time. The SBRS reported here may not be the current score for this IP address.

Parameter Name	Description
Last Sender Group	Name of the last sender group to which this IP address belonged to during the time period being reported. Note that the sender group to which an IP address belongs can change over time. The sender group reported here may not be the group to which the IP address currently belongs.
Total Attempted	Total attempted messages (recipients) for this IP address
Stopped by Reputation Filtering	Messages stopped by Reputation Filtering from this IP address.
Stopped as Invalid Recipients	Number of recipients rejected from this IP address due to invalid recipients identified by conversational LDAP acceptance or RAT restrictions.
Spam Detected	Number of messages (recipients) from this IP address identified as spam or suspect spam
Virus Detected	Number of messages (recipients) from this IP address identified as virus positive
Stopped by Content Filter	Number of messages (recipients) from this IP address that triggered at least one content filter with an action of drop, bounce, or quarantine
Total Threat	Total threat messages from this IP address
Clean	Total clean messages from this IP address

### Incoming Network Owners

GUI Page containing 'Export' link: 'Incoming Mail: Network Owners'

Parameter Name	Description
Network Owner (*)	Name of the network owner
Total Attempted	Total attempted messages (recipients) for this network owner
Stopped by Recipient Throttling	Number of recipient messages stopped as a result of HAT limits

Parameter Name	Description
Stopped by Reputation Filtering	Messages stopped by Reputation Filtering from this network owner. Includes the number of recipients stopped by recipient throttling
Stopped as Invalid Recipients	Number of recipients rejected from this network owner due to invalid recipients identified by conversational LDAP acceptance or RAT restrictions.
Spam Detected	Number of messages (recipients) from this network owner identified as spam or suspect spam
Virus Detected	Number of messages (recipients) from this network owner identified as virus positive
Stopped by Content Filter	Number of messages (recipients) from this network owner that triggered at least one content filter with an action of drop, bounce, or quarantine
Connections Rejected	Total connections rejected from this network owner
Connections Accepted	Total connections accepted from this network owner
Total Threat	Total threat messages from this network owner
Clean	Total clean messages from this network owner

## Sender Group Details

### Sender Group Connection Numbers

GUI Page containing 'Export' link: 'Sender Groups'

Parameter Name	Description
Sender Group (*)	Name of the sender group
Total Connections	Total connections that matched this sender group.

**Sender Group Mail Flow Policy Overview**

GUI Page containing 'Export' link: 'Sender Groups'

Parameter Name	Description
Accept	Total connections that triggered an 'Accept' mail flow policy action
Relay	Total connections that triggered a 'Relay' mail flow policy action
Reject	Total connections that triggered a 'Reject' mail flow policy action
TCP Refuse	Total connections that triggered a 'TCP Refuse' mail flow policy action

**Internal Users**

**Internal User Mail Flow Overview**

GUI Page containing 'Export' link: 'Internal Users'

Parameter Name	Description
Internal User (*)	Email address of an internal user.
Incoming Spam Detected	Number of incoming messages (recipients) identified as spam or suspect spam for this user
Incoming Virus Detected	Number of incoming messages (recipients) identified as virus positive for this user
Incoming Content Filter Matches	Total incoming messages (recipients) that triggered at least one content filter
Incoming Stopped by Content Filters	Total incoming messages (recipients) that triggered at least one content filter with an action of drop, bounce, or quarantine
Incoming Clean	Total clean incoming messages (recipients) for this user
Outgoing Virus Detected	Number of outgoing messages (recipients) identified as virus positive for this user
Outgoing Content Filter Matches	Total outgoing messages (recipients) that triggered at least one content filter

Parameter Name	Description
Outgoing Stopped by Content Filters	Total outgoing messages (recipients) that triggered at least one content filter with an action of drop, bounce, or quarantine
Outgoing Clean	Total clean outgoing messages (recipients) for this user

#### Individual User Detail - Incoming Mail

GUI Page containing 'Export' link: 'Internal User: <email\_address>'

Parameter Name	Description
Key (Internal User) (*)	Name of the specific internal user
Spam Detected	Number of incoming messages (recipients) identified as spam or suspect spam for this user
Virus Detected	Number of incoming messages (recipients) identified as virus positive for this user
Stopped by Content Filters	Total incoming messages (recipients) that triggered at least one content filter with an action of drop, bounce, or quarantine
Clean	Total clean incoming messages (recipients) for this user
Total Incoming Messages	Total incoming messages (recipients) for this user

#### Individual User Detail - Outgoing Mail

GUI Page containing 'Export' link: 'Internal User: <email\_address>'

Parameter Name	Description
Key (Internal User) (*)	Name of the specific internal user
Virus Detected	Number of outgoing messages (recipients) identified as virus positive for this user
Stopped by Content Filters	Total outgoing messages (recipients) that triggered at least one content filter with an action of drop, bounce, or quarantine

Parameter Name	Description
Clean	Total clean outgoing messages (recipients) for this user
Total Outgoing Messages	Total outgoing messages (recipients) for this user

**Individual User Detail - Incoming Filter Matches**

GUI Page containing 'Export' link: 'Internal User: <email\_address>'

Parameter Name	Description
Key (Internal User) (*)	Name of the specific internal user
Content Filter Name	Name of an incoming content filter configured on the system
Number of Messages	Number of incoming messages (recipients) for this internal user that triggered the above content filter

**Individual User Detail - Outgoing Filter Matches**

GUI Page containing 'Export' link: 'Internal User: <email\_address>'

Parameter Name	Description
Key (Internal User) (*)	Name of the specific internal user
Content Filter Name	Name of an outgoing content filter configured on the system
Number of Messages	Number of outgoing messages (recipients) for this internal user that triggered the above content filter

**Content Filters**

**Content Filters Summary - Incoming Filters**

GUI Page containing 'Export' link: 'Content Filters'

Parameter Name	Description
Content Filter Name (*)	Name of an incoming content filter
Number of Messages	Number of incoming messages (recipients) that triggered the above content filter



**Content Filters Summary - Outgoing Filters**

GUI Page containing 'Export' link: 'Content Filters'

Parameter Name	Description
Content Filter Name (*)	Name of an outgoing content filter
Number of Messages	Number of outgoing messages (recipients) that triggered the above content filter

**Incoming Content Filter Detail - Total Matches**

GUI Page containing 'Export' link: 'Incoming Content Filter: <Name>'

Parameter Name	Description
Key (Content Filter Name) (*)	Name of the specific incoming filter being examined
Number of Messages	Number of incoming messages (recipients) that triggered this filter during a specific time interval

**Outgoing Content Filter Detail - Total Matches**

GUI Page containing 'Export' link: 'Outgoing Content Filter: <Name>'

Parameter Name	Description
Key (Content Filter Name) (*)	Name of the specific outgoing filter being examined
Number of Messages	Number of outgoing messages (recipients) that triggered this filter during a specific time interval

**Incoming Content Filter Detail - Matches Per User**

GUI Page containing 'Export' link: 'Incoming Content Filter: <Name>'

Parameter Name	Description
Key (Content Filter Name) (*)	Name of the specific incoming filter being examined
Internal User Name	Name of a specific internal user with at least one incoming message that matched the above content filter

Parameter Name	Description
Number of Messages	Number of incoming messages (recipients) for the above internal user that matched the content filter being examined

#### Outgoing Content Filter Detail - Matches Per User

GUI Page containing 'Export' link: 'Outgoing Content Filter: <Name>'

Parameter Name	Description
Key (Content Filter Name) (*)	Name of the specific outgoing filter being examined
Internal User Name	Name of a specific internal user with at least one outgoing message that matched the above content filter
Number of Messages	Number of outgoing messages (recipients) for the above internal user that matched the content filter being examined

## Virus Outbreak Filters

#### Virus Outbreak Filter Details

GUI Page containing 'Export' link: 'Outgoing Content Filter: <Name>'

**Note** — This table does **not** contain the four timestamp columns.

Parameter Name	Description
Outbreak Name (*)	Name of a virus outbreak
Outbreak ID (*)	Outbreak ID for the above virus outbreak
First Seen Globally (UNIX Epoch Timestamp)	Seconds since the Unix Epoch when the above virus outbreak was first observed globally
Protection Time	Protection time (in seconds) provided by IronPort Virus Outbreak Filters
Quarantined Messages	Total messages released from the local VOF quarantine