Reporting API

This document provides an overview of the IronPort appliance's Reporting API feature, the information necessary to retrieve reporting data, a description of the data available through the API, and important calculations that can be made with this data.

The following topics are described:

Note — This is preview release of the feature, meant for customer feedback, and is likely to change.

REPORTING API OVERVIEW

The Reporting API feature allows you to download the same data collected by the Mail Flow Monitor component of the IronPort appliance in a comma separated value (CSV) format. The exported data can be limited by specifying date ranges, IP addresses, and frequency intervals. This format allows users to integrate the IronPort appliance's data gathering capabilities into other IT and business reporting systems.

DOWNLOADING REPORTING DATA

The reporting CSV data is available for retrieval by using an specially formatted http URL. You can retrieve mail flow data in CSV format from your IronPort appliance via http or https.You can specify limiting parameters after the '?'. If no parameters are specified, a default set of data is returned, equal to the data gathered during the previous sixty minutes plus any fraction of the current hour, reported on the minute interval.

We recommend that you create a low privilege user account on the IronPort appliance to use for retrieval of this information.

The basic format for the retrieval URL is:

protocol`://`*username*`:`*password*`@`*hostname*`:`*port*`/csv/mailflow_csv?interval=interval;startTime=`*start_time*`;endTime=`*end_time*`;remoteIPlowStr=`*low_ip*`;remoteIPhighStr=`*high_ip*

Example:

```
https://username:password@mga.company.com:8080/csv/
mailflow_csv?interval=minute;startTime=09/08%2010:00;endTime=09/
09%2015:00;remoteIPlowStr=192.168.1.1;remoteIPhighStr=192.168.100.0
```

- Whitespace in the URL should be escaped with '%20'.
- If the URL used in conjunction with a UNIX shell client (such as `wget`), all semicolons must be escaped with a "\".

Refer to Table 1-1 for a description of the user-supplied variables included in the retrieval URL.

Table 1-1 CSV URL Variables

Variable	Description
`<protocol>`	The protocol used to submit the request - http or https.
`<username>`	The user name used to log on to the host. This variable may be required depending on the browser and or protocol
`<password>`	The password used to log on to the host. The variable is optional, depending on protocol/browser/retrieval considerations.

Table 1-1 CSV URL Variables

<port>	The alternate port designation used to log on to the host. The variable is optional, depending on protocol/browser/retrieval considerations. This variable is optional.
<hostname>	The domain name or IP address of the IronPort appliance.
<interval>	The time interval - 'minute', 'hour', 'day'. This variable is optional.
<start_time>	Specifies the start time for logs to included. **[mm/dd[/yyyy]] HH:MM** if interval = 'minute' or 'hour'. **[mm/dd[/yyyy]]** if interval is "day". This variable is optional.
<end_time>	Specifies the end time for logs to include in the .csv file. **[mm/dd[/yyyy]] HH:MM** if interval = 'minute' or 'hour'. **[mm/dd[/yyyy]]** if interval is "day". This variable is optional.
<low_ip>	Specifies the low end of IP addresses to include This is the lowest IP address returned in the remoteIP column. This variable is optional.
<high_ip>	Specifies the high end of IP addresses to include . This is the lowest IP address displayed in the remoteIP column. This variable is optional.

Note **— If an IP range is not specified in the retrieval URL's** `remoteIPlowStr= and remoteIPhighStr=` variables, a "TOTAL" record (total for all IPs) is returned in the primaryDomain column, in addition to all other records. If an IP range is specified using these variables, a "TOTAL" record is not returned, but you can add all reported rows.

REPORTING DATA DESCRIPTIONS

Table 1-2 contains a list and description of the columns included in the .csv file.

Table 1-2 CSV column descriptions

Parameter Name	Description
timeStamp	Seconds since the Unix Epoch at the beginning of the measurement interval.
StartTime	The human readable time stamp at the beginning of the measurement interval.
primaryDomain	The primaryDomain is derived from the FQDN of the sending host.
remoteIP	The IP address of the remote host connecting to the MGA.
localIP	The IP address of the MGA.
recipientsIn	Number of RCPT TO commands accepted.
recipientRejectsIn	Number of RCPT TO commands rejected, due including conversational LDAP or RAT restrictions.
RATrecipientRejectsIn	Number of RCPT TO commands rejected by RAT.
tooManyrecipientRejectsIn	Number of RCPT TO commands rejected by recipient limit (from rate limiting or DHAP protection).
messagesIn	Number of SMTP DATA commands (messages) accepted.
bytesIn	Total bytes received, excluding SMTP protocol messages.
connectionAcceptsIn	Number of successful inbound connections.
spamSuspectMsgsIn	The number of suspected spam messages.
connectionRejectsIn	Number of inbound connections rejected.
starttlsSuccessesIn	Inbound STARTTLS commands successfully processed.
starttlsFailuresIn	TLS failures after STARTTLS command received.
recipientsOut	RCPT TO commands that succeeded.
recipientRejectsOut	RCPT TO commands that were rejected.

Table 1-2 CSV column descriptions (Continued)

messagesOut	SMTP DATA sent and server responded “OK”.
BytesOut	Total bytes sent, excluding SMTP protocol messages.
connectionAcceptsOut	The number of times the MGA successfully establishes a client (outbound) SMTP session.
connectionFailuresOut	Outbound connection setup failures (in TCP).
connectionRejectesOut	Outbound connections established then rejected.
starttlsSuccessesOut	STARTTLS commands that established a secure connection.
starttlsFailuresOut	STARTTLS commands that failed.
SenderBaseOrgID	Sender Base Organization ID of the connecting IP address.
SenderBaseReputationScore	The most recent Sender Base Reputation Service score for the connecting IP address.
senderGroup	The most recent sender group that the connecting IP address matched.
senderPolicy	The mail flow policy applied to the connecting IP address.
spamScanMsgsIn	The number of rcptacess scanned by the anti-spam engine. (This counts the number of recipients in a message)
spamFoundMsgsIn	The number of messages (number of recipients in message) found to be spam-positive. (This does not include suspected spam.)
virusFoundMsgsIn	Number of messages (number of recipients in message) found to contain a virus.

Table 1-2 CSV column descriptions (Continued)

virusScanMsgsIn	Number of messages (number of recipients in message) scanned for viruses.
workDequeues	Number of messages (number of recipients in message) submitted into the scanning pipeline (filters, anti-spam, anti-virus).
recipientsUnknownIn	Total recipients received from sending IP addresses that do not match defined sender groups.

MAIL FLOW MONITOR CALCULATIONS

Mail Flow Monitor uses the values in the reporting database to calculate the numbers presented in the Monitor tab of the IronPort Appliance's GUI, as well as in the scheduled reports you can configure for regular delivery.

The following section describes how to calculate, from the CSV columns, values displayed in the Inbound Mail Summary, the 'Basic' view of the Domain Detail Table and in the Incoming Mail Overview Scheduled Report.

Attempted Messages

The total number of attempted messages is equal to the number of inbound connections rejected times a standard factor plus the number of RCPT TO commands rejected plus the number of messages sent to the work queue.

Attempted Messages In = (3 * connectionRejectsIn) + recipientRejectsIn + workDequeques

For more information about the multiplier used in this calculation, please see the note following this section.

Stopped by Reputation Filtering

The number of messages stopped by sender reputation includes recipient messages rejected based on information derived from the sender IP address. This total includes an estimate of recipients that would have been sent but were prevented due to a rejection of the connection because the IP address fell into a sender group with a 'reject' action. This includes recipients rejected because the IP address was in a throttled sender group for which the recipient limit was exceeded.

Stopped by Reputation Filtering = (3 * connectionRejectsIn) + toomanyRecipientRejectsIn

For more information about the impeller used in this calculation, please see the note following this section.

Invalid Recipients

The number of invalid recipients is equal to the number of recipients rejected (listed in the RAT or not accepted by conversational LDAP) minus the number of recipients rejected due to rate limiting.

Invalid Recipients = recipientRejectsIn - tooManyrecipientRejectsIn

Total Spam Messages Detected

The total number of spam messages detected is equal to the number of spam-positive messages plus the number of spam-suspect messages.

Total Spam Messages Detected = spamFoundMsgsIn + spamSuspectMsgsIn

Total Virus Messages Detected

The total number of virus-positive messages is equal to virusFoundMsgsIn.

Total Virus Messages Detected= virusFoundMsgsIn

Total Threat Messages

The total number of messages containing threats is equal to the sum of messages rejected by sender reputation, other recipient rejects, spam positive messages, and virus positive messages.

Total Threat Messages = reputationRejectsIn + invalidRecipientsIn

+ spamAndSuspectIn +virusFoundMsgsIn

Clean Messages Accepted

The number of clean messages accepted is equal to total number of recipient messages minus the sum of recipient messages included in all other categories (spam messages and virus positive messages). This number does not include messages that were dropped by message filters or messages that were quarantined by Virus Outbreak Filters.

Clean Messages Accepted = workDequeues - (spamFoundMsgsIn + spamSuspectMsgsIn) - virusFoundMsgsIn

Note — The impeller of three ("3"), used in several of these calculations, addresses the fact that messages blocked by reputation filtering do not actually enter the work queue. Due to this, the appliance does not have access to the list of recipients for an incoming message and needs to estimate the number of recipients. This hard-coded multiplier was determined by IronPort Systems, Inc. and is based upon research of a large sampling of existing customer data.