Reporter 10.x
Administrator Guide
This document describes the functionality of Blue Coat® Reporter 10.x.

This document provides the following:

- Describes the Reporter network footprint.
- How to manage Reporter user access.
- How to monitor Reporter operations.
- How to solve problems.

Table Of Contents

Blue Coat Reporter 10.x Administrator Guide .................................................. 3
Table Of Contents ................................................................................................. 3
About Reporter Licensing ......................................................................................... 9
  Reporter RP-S500 Appliance ................................................................. 9
  Reporter VA .............................................................. 9
  Reporter VA—About the Phone-Home Service ............................................. 9
About Reporter Architecture ................................................................................. 10
  Related Conceptual Information ................................................................. 11
About Log Processing ......................................................................................... 12
  Overview ................................................................................................. 12
  About Optimizing Log Processing Configurations ...................................... 12
    About the Decimal Digits ........................................................................ 12
About the Page View Combiner ........................................................................... 15
  Requirements ............................................................................................. 16
  Additional Reference ............................................................................... 16
Reporter Resource Sizing .................................................................................... 17
  FTP Servers ................................................................. 17
  RP-S500 Appliances .............................................................. 17
# Table of Contents

- **Virtual Appliances** .................................................................................. 17
- **Manage Access** ...................................................................................... 18
- **About Users** ......................................................................................... 18
  - Admins ................................................................................................... 18
  - Standard User ........................................................................................ 18
- **About Roles** .......................................................................................... 18
- **About Role-Based Access** ....................................................................... 19
  - Plan the Roles ......................................................................................... 20
  - LDAP Group-Based Option ..................................................................... 20
  - Define a Role .......................................................................................... 21
- **Create a New Reporter User** .................................................................. 22
  - Specify the Connection Duration ............................................................ 22
  - Related Step ............................................................................................ 22
- **Define a User or Group Role** ................................................................. 23
- **About LDAP Integration** ....................................................................... 25
  - About Nested Groups ............................................................................ 25
  - Begin Walkthrough? ............................................................................... 26
- **Connect to LDAP Server** ...................................................................... 27
  - Prerequisites ........................................................................................... 27
  - Procedure ................................................................................................ 27
  - Next Step ................................................................................................ 29
- **Assign Roles From LDAP** ................................................................. 30
  - Prerequisite ............................................................................................ 30
  - Procedure ................................................................................................ 30
- **Administrative Tasks** ......................................................................... 31
  - Recommended Tasks ............................................................................... 31
  - CLI ........................................................................................................... 31
  - Other Tasks ............................................................................................. 31
- **Connect Reporter to Email Server** ..................................................... 33
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisite</td>
<td>33</td>
</tr>
<tr>
<td>Procedure</td>
<td>33</td>
</tr>
<tr>
<td>Email Alerts to Administrator</td>
<td>35</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>35</td>
</tr>
<tr>
<td>Procedure</td>
<td>35</td>
</tr>
<tr>
<td>Monitor Reporter Operations</td>
<td>36</td>
</tr>
<tr>
<td>System Overview</td>
<td>36</td>
</tr>
<tr>
<td>System Resources</td>
<td>36</td>
</tr>
<tr>
<td>Database Overview</td>
<td>36</td>
</tr>
<tr>
<td>View Archived Reports</td>
<td>37</td>
</tr>
<tr>
<td>View Scheduled Tasks</td>
<td>37</td>
</tr>
<tr>
<td>Manage Existing Databases</td>
<td>38</td>
</tr>
<tr>
<td>Database</td>
<td>38</td>
</tr>
<tr>
<td>Log Source</td>
<td>39</td>
</tr>
<tr>
<td>Change the Reporter Interface Language</td>
<td>42</td>
</tr>
<tr>
<td>Support Languages</td>
<td>42</td>
</tr>
<tr>
<td>How Do I?</td>
<td>42</td>
</tr>
<tr>
<td>Convert International Domain Names</td>
<td>43</td>
</tr>
<tr>
<td>Change an Admin Password</td>
<td>44</td>
</tr>
<tr>
<td>Notes</td>
<td>44</td>
</tr>
<tr>
<td>Procedure</td>
<td>44</td>
</tr>
<tr>
<td>Set Reporter Email From Value</td>
<td>45</td>
</tr>
<tr>
<td>Reference: CLI</td>
<td>46</td>
</tr>
<tr>
<td>Basic Commands</td>
<td>46</td>
</tr>
<tr>
<td>Enable Mode Commands</td>
<td>46</td>
</tr>
<tr>
<td>Reference: Log Fields</td>
<td>49</td>
</tr>
<tr>
<td>Reference: Web API Parameter Syntax</td>
<td>56</td>
</tr>
<tr>
<td>Common Parameters</td>
<td>56</td>
</tr>
<tr>
<td>Description</td>
<td>56</td>
</tr>
</tbody>
</table>
Example .................................................................................................................. 56
Description ............................................................................................................... 56
Example .................................................................................................................. 56
Description ............................................................................................................... 56
Example .................................................................................................................. 56
Description ............................................................................................................... 56
Example 1 ................................................................................................................ 57
Example 2 ................................................................................................................ 57

End Point: /api/create ............................................................................................. 57
Example—One-level summary report; archived to server ........................................ 58
Example—Two-level summary report; sorted, filtered, and archived to server ....... 58
Description ............................................................................................................... 58
Example .................................................................................................................. 58
Description ............................................................................................................... 59
Example .................................................................................................................. 59
Description ............................................................................................................... 59
Example .................................................................................................................. 59
Description ............................................................................................................... 59
Example .................................................................................................................. 59
Description ............................................................................................................... 59
Value Syntax ........................................................................................................... 59
Examples ................................................................................................................ 59
Description ............................................................................................................... 60
Examples ................................................................................................................ 60
Description ............................................................................................................... 60
Examples ................................................................................................................ 60
Description ............................................................................................................... 60
Examples ................................................................................................................ 60
Description ............................................................................................................... 60
Examples ................................................................................................................ 60
Description ............................................................................................................... 61
Examples ................................................................................................................ 61
End Point: /api/status ................................................................. 64
  Required Parameters ......................................................... 64

End Point: /api/cancel ............................................................. 64
  Required Parameters ......................................................... 64

End Point: /api/download ....................................................... 64
  Required Parameters ......................................................... 64

End Point: /api/listDatabases .................................................. 64
Required Parameters ................................................................. 64
End Point: /api/listFields .......................................................... 64
  Required Parameters ............................................................ 65
Debugging ............................................................................... 65
Relative Dates ................................................................. 66
  Examples ........................................................................ 66
Trend Reports ................................................................. 67
  Diagnose Reporter ............................................................. 68
    Symptom .................................................................... 68
    Scenarios .................................................................... 68
    Workaround ................................................................. 68
About Reporter Licensing

The Blue Coat Reporter limits the maximum disk space the product uses. Blue Coat provides the following Reporter 10.x license options.

**Reporter RP-S500 Appliance**

The license matches the total disk space (original specification). Check the current System Resources consumption on the Admin link > System Overview > System Diagnostics page.

**Reporter VA**

Blue Coat offers licenses, which allows up to the total usable disk space.

- RP-V50
- RP-V100
- RP-V200

Each versions specifies CPU and RAM sizing. For a complete sizing schematic, see "Reporter Resource Sizing" on page 17.

**Reporter VA—About the Phone-Home Service**

The following information applies to Reporter VA only.

To ensure license integrity, Reporter VA periodically communicates with Blue Coat license portal to validate the issued licenses. This requires continuous successful network connectivity with the Blue Coat network. To allow for temporary WAN outages, this operation continues for 12 hours or until a successful license validation occurs. After 12 hours, the Reporter license state changes to invalid. Until this license issue is resolved, you can continue to use all Reporter functionality except for new database and log source creation; furthermore, Reporter halts the processing of all new data in existing databases.

Because of the Phone-Home Service, Reporter VA is not supported in closed networks. For that deployment scenario, consider the Reporter appliance (RP-S500), which employs a licensing scheme based on unique hardware serial numbers. Blue Coat expects to release this platform in early Fall, 2015.
**About Reporter Architecture**

Blue Coat Reporter is a key component in the Secure Web Gateway solution. Reporter generates and displays reports based on web traffic access log data that is sent from one or more gateway ProxySG appliances. Analyzing reports gives insight regarding the integrity of the network and user web browsing habits and policy compliance.

This allows you to:

- Identify possible security threats (such as malware/spyware).
- View user activity by user, group, URLs, or other aspect.
- View blocked web traffic (such as categories and URLs).
- Identify which users consume how much network bandwidth from web use.

A—Employees perform web content requests.
B—The gateway ProxySG appliance records transactions and uploads access logs to a dedicated FTP server.

C—The Reporter device (appliance or VA), retrieves the data from the FTP server—the defined log source—and populates the defined database. More than one log source can feed a database (for example, multiple locations). Reporter users (admins and users with role-based access) generate and view reports.

The initial Reporter release, 10.1.2, is only available on the VA platform. Furthermore, Reporter VA is not supported in closed networks. If you require more information, see About Reporter Licensing on page 9.

D—Based on trends viewed in the reports, admins adjust the web-use and security polices on the gateway Proxy appliance.

Reporter performs the following major tasks.

- Processes raw log data received from ProxySG appliances and populates databases.
- Manages the databases and generates reports.
- Manages the Reporter appliance/VA functions.

Related Conceptual Information

- "About Log Processing" on page 12
- "About the Page View Combiner" on page 15
- About the Default Browse Time Calculations
About Log Processing

Overview

Log processing involves the following components.

- **Log Reader**—Reads access log data into Reporter memory.
- **Page View Combiner (PVC)**—This sub-component of the log reader attempts to provide more realistic user browsing statistics by combining the initial request and its secondary referral requests as one page count. For detailed information about the PVC, see About the Page View Combiner on page 15.
- **Log Processor**—Populates the databases with the log data.

About Optimizing Log Processing Configurations

This section describes some conditions that affect log processing efficiency.

About Access Log Naming Conventions

This section provides suggestions for ProxySG appliance access log naming conventions, especially for deployments that require processing a large number of log files over a longer duration of time.

For optimal Reporter performance, configure your access logs to use the following filename format:

```
xxxxxxxxxxxxxxxxNddddddddd..log.gz
```

where:

- x represents any valid character that can be used in naming a log file (letters, digits, underscore, dash).
- N represents a non-decimal-digit character.
- d represents a decimal digit. This number, preceding the log file extension, determines the order in which the log files are processed. The log file ordering is performed identically for FTP and local disk log sources. A date string representing the log line dates within the file is preferred. If you mix cloud files with on-premise files, use the 12-digit cloud date syntax described above.
- .log.gz is the extension of the (compressed) log file.

About the Decimal Digits

The decimal digit number is the key part of the format.

- If this number does not provide a complete ordering on the set of log files, then the log processing speed suffers because of internal log table thrashing.
- A filename format of MMDDhhmmss is inadequate because the files process chronologically, except at year-end when they temporarily process out-of-order because of the December (MM = 12) rollover into January (MM = 01) where January files sort before December.
A filename format of hhmmss is more problematic because log files are processed out-of-order whenever one day rolls into the next.

- Given these constraints, to ensure the most efficient log file ordering, format this eleven-digit number as: YYJJJhhmmss, where:
  - YY = two-digit year (00 - 99)
  - JJJ = three-digit Julian day of the year (001 - 366)
  - hh = two-digit hour of the day (00 - 23)
  - mm = two-digit minute of the hour (00 - 59)
  - ss = two-digit second of the minute (00 - 59)

  Using this format allows Reporter to properly order log files through the year 2021.

- The default filename format used for log files on the ProxySG appliance has the following text and specifiers: SG_%f_%c_%l%m%d%yj%H%M%S.log.gz.
  - %f = log name (facility)
  - %c = name of the external certificate used for encryption, if any
  - %l = the fourth parameter of the ProxySG appliance IP address (101.102.103.104)
  - %m = two-digit month (01 - 12)
  - %d = two-digit day (01 - 31)
  - %h = two-digit hour (00 - 23)
  - %M = two-digit minute (00 - 59)
  - %S = two-digit second (00 - 59)
  - .log.gz = extension

  The suggested filename format for log files on the ProxySG appliance slightly alters the default and has the following text and specifiers: SG_%f_%c_%l%m%d_%yj%H%M%S.log.gz.
  - %y = two-digit year, without century (00 - 99)
  - %j = three-digit Julian day within year (001 - 366)

  The value of this naming convention for log files is very evident when processing large numbers of log files (spanning multiple days and months) occurs. The value is less evident when log file generation and processing occurs regularly (daily or more frequently) so that out-of-order files occur infrequently. However, when re-processing large sets of log files, the naming convention is essential.

About Chronological Ordering

Each database creates and manages its own memory resident Log Table. Each Log Table is comprised of hour-tables containing data for each hour the database Log Processors spend reading log files. These tables constitute some of the most active memory in Reporter, and therefore have a significant impact on overall log processing performance. If all log files were processed in chronological order, there would never be more than one hour-table necessary in memory. It is common for the log processing process to encounter batches of log files spanning multiple hours between them. If they are processed out of chronological order, performance significantly improves by allowing the number of hour-tables to grow,
provided there is sufficient process memory. Conversely, during low memory conditions, reducing the number of hour-
tables prevents unnecessary memory starvation and subsequent disk operations (swapping files in and out of memory).

Reporter orders log files based on a numeric field in the filename, when it is present. The default filenames created by the
ProxySG contain a Month/Day/Hour/Minute/Second timestamp immediately preceding the .log or .log.gz suffix; for example: SG_Main_HQ-1_1102081500.log.gz. If the filename ends with .log or .log.gz, the Log Processor parses it for any purely numeric sequence immediately preceding the required suffix. If one is found, it is then used to sequentially order that batch of log files. You can significantly improve Log Processor performance by naming the log files with any ordered numeric values that comply with this format. For example: anyfilenameprefix123.log or some-other-prefix-84757.-log.gz.

**About Database Purging**

Most of the database is kept in memory. If the entire database is not occasionally purged, it would continue to consume
more of the process memory as new log files are processed. As the database grows, configuration settings that were pre-
viously beneficial might become detrimental.

As a general guideline, Blue Coat recommends that databases contain a maximum of 30 days of log data. However, the
amount of log data is more relevant than the number of days in the data sets.

Reporter also allows the administrator to purge the database based on the number of log lines. Purge the log lines by expir-
ation, automatically (scheduled), or manually.
About the Page View Combiner

The Page View Combiner (PVC) is called during Blue Coat Reporter log processing. The PVC combines multiple HTTP requests that are associated with a single web page into a single log line. When a user browses to a web page, most often that page triggers requests for more content, either from the same web server or another server (for example, a media server that stores video or image content). Rather than regard each of these as separate requests, the PVC combines all of the bytes into the original request.

The goals of the PVC are to:

- Reduce the number of database entries from the original log file, which improves report generation performance.
- More closely represent user browsing activity, as each object (requested by the first page from content servers) is not counted as a separate entry.
A—An Employee performs web content request from **www.example.com**.

B—The example.com server S1 sends additional requests to other servers in its farm for advertisements and video content and receives four data objects.

- example.com/main.html
- i.example.com/ads/sponsor1.gif
- example.com/news/story1.html
- example.com/news/video1

C—The gateway ProxySG appliance adds access log entries for all of these content elements.

D—The Reporter PVC combines the log lines into one page view and saves that in the database. The Reporter users generates and views a report that contains one page view entry for the original request to **www.example.com**.

It is possible that a web request that would normally be combined to represent one page view might be split into two page views. This occurs when, as a result of internal processing, the log sources are halted or restarted or the request is recorded across two log files.

If this occurs, no data is lost, but the database contains two page views. Continuing with the example in the previous illustration:

```
8:40:20 cnn.com/html
8:40:20 i.cnn.com/ads/sponsor1.gif
[-------end of log file----------]
[----beginning of new log file-----]
8:40:21 cnn.com/news/video1.asf
```

The first two entries are shown as one page view; the second two as another within the database. However, they represent a single page view requested by a user.

**Requirements**

The PVC requires the following fields in the logs:

- cs-referer
- sc-status
- rs(Content-Type)

The Blue Coat-recommended log formats contain these fields (see also Reference: Log Fields on page 49).

If these log fields are not present, no page-view combining occurs, and report data represents each and every web request.

HTTPS logs do not contain the sc-status field; therefore, PVC calculations cannot occur. The field is not included because it would expose personal user data (such as bank account information).

**Additional Reference**

- See Reference: Log Fields on page 49.
Reporter Resource Sizing

This section provides the supported server information required to operate Reporter.

FTP Servers

Blue Coat Reporter requires a ProxySG appliance to send its bcreportermain format access logs to a dedicated FTP server.

These are the FTP server types with which Blue Coat has tested Reporter. Other FTP servers might function correctly, but they are not officially supported by Blue Coat.

- Windows FTP (through IIS)
- Linux: VSFTPD

RP-S500 Appliances

- 24TB
- RAID 10
- 262144 RAM
- 40 CPU

Virtual Appliances

Blue Coat Reporter is supported on ESXi 5.5 Update 2 (minimum build: 2068190) virtual appliances with ESX Enterprise or Enterprise Plus licenses (the Basic license does not allow enough processing resource). The purchased license determines how many CPUs and how much RAM are required to ensure that Reporter processes run efficiently. Use this data to understand how much resource to dedicate.

<table>
<thead>
<tr>
<th>VA License</th>
<th>CPUs</th>
<th>Minimum Memory</th>
<th>Maximum Drive Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP-V50</td>
<td>8 cores</td>
<td>65536 MB</td>
<td>2200</td>
</tr>
<tr>
<td>RP-V100</td>
<td>16 cores</td>
<td>131072 MB</td>
<td>4400</td>
</tr>
<tr>
<td>RP-V200</td>
<td>32 cores</td>
<td>196608 MB</td>
<td>8800</td>
</tr>
</tbody>
</table>

For more information about licensing, including product behavior when a license is not valid, see "About Reporter Licensing" on page 9.
Manage Access

Reporter classifies three types of users who can access the Management Console.

About Users

Admins

- **Default Administrator**—This is the Reporter administrator account that is created when Reporter is installed. The default administrator has access to all Reporter functions, including administration options and all reports. This user can be deleted by another administrator, but a user cannot delete themselves, and the last administrator on the system cannot be deleted.

- **Administrator**—The default administrator can create additional administrator users. Like the default administrator, these users have access to all Reporter functions, including administration options and all reports.

Standard User

A standard user who logs into Reporter has access to the report databases to which they are assigned. Standard users do not have access to the **Administration** link, but they can change their Reporter access password and e-mail identity.

Proceed to "Create a New Reporter User" on page 22.

About Roles

Reporter allows you to create role-based access control. You can manually assign users to a role or integrate your LDAP active directory.

Proceed to one of the following to learn more.

- "About Role-Based Access" on the next page.
- "About LDAP Integration" on page 25.
Roles allow you, the Reporter administrator, to restrict non-admin Reporter user access to a limited report set. Typically, non-admin Reporter users are IT or HR professionals within an enterprise. IT specialists likely monitor network health and performance, while HR personnel monitor employee acceptable web use. When you give such users access to Reporter, you might elect to limit them to report types that fit their roles.

A role is defined as access to database fields. Your Reporter deployment contains at least one database and likely has multiple. Access logs from a gateway ProxySG appliance populate databases from which Reporter generates the reports. The report data is defined by database fields. For example, the Content-Type field indicates the type of media served in the transaction. Therefore, you define a role by assigning which database fields are viewable.

To define roles, you must understand what database field provides what data type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Suggested Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Protocol communication action between client and server (tcp_miss, tcp_hit).</td>
<td>IT</td>
</tr>
<tr>
<td>Category</td>
<td>Browsed web content category.</td>
<td>HR</td>
</tr>
<tr>
<td>Cert Svr Domain</td>
<td>The name of the entity that was authenticated. For example, <a href="http://www.example.com">www.example.com</a>.</td>
<td>IT</td>
</tr>
<tr>
<td>Certificate Category</td>
<td>The authentication category to which a certificate belongs.</td>
<td>IT</td>
</tr>
<tr>
<td>Certificate Error</td>
<td>The type of error that caused a problem with a certificate or the server's use of the certificate.</td>
<td>IT</td>
</tr>
<tr>
<td>Cipher Strength</td>
<td>The code for the number of bits used to encrypt web traffic (HTTPS).</td>
<td>IT</td>
</tr>
<tr>
<td>Client IP</td>
<td>The IP address of the user's system.</td>
<td>IT</td>
</tr>
<tr>
<td>Content Type</td>
<td>The type of web media served; for example, PDF file.</td>
<td>IT</td>
</tr>
<tr>
<td>Group</td>
<td>The (enterprise-defined) group to which the user belongs; for example, Finance or Engineering.</td>
<td>HR, IT</td>
</tr>
<tr>
<td>Log Source</td>
<td>The IP address of the ProxySG appliance that sent the log files.</td>
<td>IT</td>
</tr>
<tr>
<td>Malware</td>
<td>The name of any type of malware, spyware, or other malicious code encountered by users</td>
<td>IT</td>
</tr>
<tr>
<td>Method</td>
<td>Limit set of browser methods, such as GET, POST, and HEAD.</td>
<td>IT</td>
</tr>
<tr>
<td>Port</td>
<td>The port over which web content arrived.</td>
<td>IT</td>
</tr>
<tr>
<td>Protocol</td>
<td>The transport protocol used to deliver web content; for example, HTTP or RTSP.</td>
<td>IT</td>
</tr>
<tr>
<td>Site</td>
<td>The name of the browsed website.</td>
<td>HR, IT</td>
</tr>
<tr>
<td>Status</td>
<td>Status response from server; for example: 200/success, 404/not_found, 503/not_available.</td>
<td>IT</td>
</tr>
<tr>
<td>User</td>
<td>The user name (requires authenticated usernames in the access logs).</td>
<td>HR</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Suggested Role</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>User Agent</td>
<td>The application that requested the web content; for example, Mozilla Firefox or QuickTime.</td>
<td>IT</td>
</tr>
<tr>
<td>Verdict</td>
<td>The policy verdict; for example, allowed or denied.</td>
<td>HR</td>
</tr>
</tbody>
</table>

**Plan the Roles**

Blue Coat recommends planning the roles before attempting to define them in Reporter. Based on the information in the previous table, you can create a matrix and follow that when you configure Reporter.

**Example**

<table>
<thead>
<tr>
<th>User</th>
<th>Group/Department</th>
<th>Location</th>
<th>Admin</th>
<th>Role Name</th>
<th>Database</th>
<th>DB Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>hub.porter</td>
<td>IT (Admin)</td>
<td>Corporate</td>
<td>Yes</td>
<td>Admin</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>jimmy.bond</td>
<td>IT; Malware &amp; Security</td>
<td>Corporate</td>
<td>No</td>
<td>IT Security</td>
<td>All</td>
<td>Client IP, Malware, Cert fields</td>
</tr>
<tr>
<td>maya.santos</td>
<td>HR; Site B HR</td>
<td>Site B</td>
<td>No</td>
<td>HR</td>
<td>San Jose</td>
<td>User, Category, Verdict</td>
</tr>
</tbody>
</table>

**Planning Form**

<table>
<thead>
<tr>
<th>User</th>
<th>Group/Department</th>
<th>Location</th>
<th>Admin</th>
<th>Role Name</th>
<th>Database</th>
<th>DB Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**LDAP Group-Based Option**

You have the option to integrate your existing LDAP active directory with Reporter, which allows you to assign Group names to roles. See "About LDAP Integration" on page 25.
Define a Role

- Proceed to "Define a User or Group Role" on page 23.
Create a New Reporter User

Any Reporter user who has administrative credentials can create new administrative and standard users. For optimal security, Blue Coat strongly recommends limiting the number of users who have administrative credentials. You can create new administrator users and standard users anytime.

If you plan to employ role-based access, consider creating new standard users after you define the roles. This is not required, however, as you can edit an existing user and assign the role.

1. On the Administration > General Settings page, select Access Control > Local Users.
2. Click New. Reporter displays the Create New User wizard.
   a. Enter the Username that the user enters to access Reporter. If you have a planning sheet with names, be sure to enter them exactly as printed. Click Next to move to the next page: Set Password.
   b. Enter a New Password, which is the access credential password for this user; repeat in the Validate Password field. Again, if you are following a planning sheet, enter the password exactly as printed. If you are creating the passwords, record them accurately. Click Next to move to the next page: Set Permissions.
   c. Select the user type.
      - **Administrator**—The user has full access to Reporter and all roles.
      - **User**—The user has limited access to Reporter. If you select this option, select the role(s) to which this user belongs (if Reporter contains defined roles).
   d. Click Done. The new user displays on the Local Users page.

Created users can now access Reporter when you give them the network address and their credentials.

Specify the Connection Duration

By default, the Reporter Management Console remains indefinitely connected for all users. For more security control, you can set a time value after which the Management Console disconnects and forces users to re-log in with their access credentials.

1. On the Administration > General Settings page, select System Settings > Server Settings.
2. In the Web Server Settings > Session Timeout area, slide the time duration bar to set the session time limit.
3. Click Save.

Related Step

Reporter allows you to define roles based on users or groups (LDAP).

- About Role-Based Access on page 19.
- "About LDAP Integration" on page 25.
- "Define a User or Group Role" on the next page.
Blue Coat Reporter allows you to restrict user access to all but the reports they require for their positions within the enterprise. In Reporter, a role is defined by access permissions to which non-admin users are assigned. These permissions can be as broad as access to an entire database or as granular as access to specific data fields within generated reports.

Defining user roles requires planning. Before creating roles, Blue Coat recommends creating a list of roles within your enterprise and a list of users who require access to specific report data. See "About Role-Based Access" on page 19 for planning information.

1. From the Reporter Management Console (logged in with administrator credentials), select **General Settings > Reporter Settings > Access Control > Roles**.
2. Click **New**; Reporter displays the Create New Role dialog.
3. Specify the role parameters.
   a. **Name** the role; the more specific the name, the easier it will be to assign your users to their correct roles. Click **Next** to move to the next page of the wizard: Permissions.
   b. Select the databases that users in this role can access.
   c. By default, the role has access to all database fields. To limit the fields that reports in this role display, clear the unnecessary field options (or select **No Fields** to clear all options, then select the required options).
   d. (Optional) To further limit report data, apply a filter to the role. For example, you want a role that is limited to report data indicating which users experienced content filtering and policy denials.
   e. Click **Done**. Reporter displays the new role on the **Roles** page.
About LDAP Integration

If your enterprise uses Lightweight Directory Access Protocol (LDAP) compatible database, you can assign LDAP groups to specific Reporter roles. This allows the security network administrator to maintain a single-source authentication directory. For example, if the LDAP database has a user group named HR, you assign the HR LDAP group to the HR role you created in Reporter. When a user from the HR group enters their username and password into Reporter, they are authenticated and allowed access to the reports you assigned to that role.

About Nested Groups

Some LDAP directories, such as Active Directory, allow a group to contain members that are also groups. When a group is a member of another group, it is called a nested group. With nested groups, the groups a user is associated with are:
Any group that the user is a member of;
Any groups those groups are a member of; and
Any groups those groups are a member of and any groups those groups are a member of.

The nesting continues for as many layers of groups exist. For example, the enterprise contains a group called Engineering, which contains members Engineering A, Engineering B, and Engineering C, all of which are also groups containing members (users). With nested groups, a member of Engineering A essentially becomes a member of Engineering. When nesting is enabled on Reporter, all members of Engineering A, Engineering B, and Engineering C have access to the role assigned to Engineering. Reporter supports nested groups; when nesting is enabled and a group is assigned to a role, users in all groups in the nest have access to the role. Enable nested group support when configuring access control.

Begin Walkthrough?

Proceed to "Connect to LDAP Server" on the facing page.
Connect to LDAP Server

Specify the Lightweight Directory Access Protocol (LDAP) that Reporter uses to authenticate users. Reporter supports Microsoft Active Directory and Novell eDirectory, with pre-configured settings. You can also create your a custom LDAP server connection.

Reporter supports multiple trees, but you must add multiple realms (each realm is used in order). If a tree contains multiple servers, no one server contains all users, and the base DN is configured at a level in the tree higher than where the servers diverge, add an additional base DN for each unique partition in the tree. Reporter requires a base DN for each partition that is not globally replicated.

Prerequisites

To configure these options, you must know:

- The IP address of the primary LDAP server (secondary optional, but recommended).
- LDAP searching access credentials (if required).
- Naming attributes.
- Base DN information.

Procedure

In Reporter on the Admin portal.


2. Select the LDAP directory system that your enterprise employs.
   - Microsoft Active Directory
   - Novell eDirectory
   - Other LDAP

   Click Next to move to the next wizard screen: Set Name.

3. Name the Realm that contains the list of users who will have access to the roles. By default, Reporter allows disconnected logins, which means that users are able to log in when Reporter is not able to connect to LDAP servers. For the highest security level, clear the Allow Disconnected Login option. Click Next to move to the next wizard screen: Set Servers.

4. Enter the LDAP server information.
a. For the **Primary** LDAP server, enter the **Host** IP address.
   
b. The default **Port** is **389**. If you select **Use SSL**, which secures the connection from the Reporter server to the LDAP server, the default port changes to **636**. If you have configured your LDAP servers to use a different port, enter it.
   
c. (Optional) Enter **Secondary Server** information. Reporter attempts to connect this server should the Primary become unavailable.
   
d. Click **Next** to move to the next wizard screen: Set Search Credentials.

5. Specify whether or not user **Credentials** are required to search the LDAP directory
   
   - **No Credentials Required**—The LDAP server does not require a password for search access.
   - **Use Credentials**—Selecting this displays more fields. Enter the LDAP server **User Name** (Fully Qualified Domain Name (FQDN)) and the password required for search access.

   Click **Next** to move to the next wizard screen: Set Naming Attributes.

6. Verify or enter the user attribute.
   
   - If you selected **Microsoft Active Directory** or **Novell eDirectory**, Reporter populates the naming attributes with default LDAP realm values. If your realm information differs, enter the correct attributes. Otherwise, click **Next** to move to the next wizard screen: Set Base DNs.
   
   - If you selected **Other LDAP**, you must enter the naming conventions that match your custom LDAP configuration, then click **Next** to move to the next wizard screen: Set Base DNs.

7. Enter all **User Base DNs** and **Group Base DNs** that are searchable. **Show screen...**
In this example, the first **User Base DN** is the default location for users in Active Directory for the example.com company. The first **Group Base DN, Builtin**, is also the default for Active Directory.

- dc= represents DNS naming in the directory. The DNS name example.com becomes dc=example,dc=com in the DC naming convention. This is the format that Active Directory uses. Typically, Base DNs are not set at a dc= level in the directory.

Click **Next** to move to the next wizard screen: Test Connection.

8. Testing the LDAP server connection is optional but recommended to verify functionality before entering into production. Click **Test LDAP Settings**. If any errors occur, click **Previous** to return to the problematic setting screen and correct the information.

Following a successful test, click **Done**.

**Next Step**

- Proceed to "Assign Roles From LDAP" on the next page.
Assign Roles From LDAP

If your enterprise uses Lightweight Directory Access Protocol (LDAP) compatible database, you can assign LDAP groups to specific Reporter roles. This allows the security network administrator to maintain a single-source authentication directory. For example, if the LDAP database has a user group named HR, you assign the HR LDAP group to the HR role you created in Reporter. When a user from the HR group enters their username and password to access Reporter, they are authenticated and allowed access to the reports that are assigned to that role.

For more information about roles, including planning information, see "About Role-Based Access" on page 19.

Prerequisite

You must configure Reporter to communicate with your LDAP servers. See "Connect to LDAP Server" on page 27.

Procedure

In Reporter on the Admin portal.

1. On the Administration > General Settings page, select Access Control > LDAP Groups.
2. Click New. Reporter displays the Create New Item wizard.
3. Reporter detects the present LDAP groups.
   a. Select an available configured LDAP group that will have permissions to access this role.
   b. (Optional) Selecting Include nested groups allows all members in the group tree to have access to this role; if this option is not selected, only members in the specified group have access to this role. For more information about nested LDAP groups, see About LDAP Integration on page 25.
   c. Click Next to move to the next wizard screen: Set Permissions.
4. Select a Permissions option.
   a. Select LDAP Group and select the roles to which this group has access; or
   b. Select Administrator to give this group full access to Reporter.
5. Click Done. The LDAP Groups page contains the new group.
After completing the Reporter initial configuration process, consider completing other configuration tasks, depending on your network and business requirements.

**Recommended Tasks**

**Prevent Denial-Of-Service Attacks**

Relating to a Blue Coat Security Advisory (https://bto.bluecoat.com/security-advisory/sa74), malicious remote clients might perform a DoS attack against OpenSSL-based servers by repeatedly renegotiating the connection. The longer connections exist, the more susceptible are they to man-in-the-middle attacks. You can configure Reporter to renegotiate SSL sessions, which prevents these attacks.

Reporter provides an option called **Force Secure Negotiation**, which is located on the General Settings > Reporter Settings > System Settings > Server Settings page.

Be advised that after this option is enabled, Reporter only supports clients that support secure renegotiation. To support older clients that do not support the secure renegotiation option, clear this option.

**Setup Email for Admin Alerts and User Reports**

Two Reporter functions require you to setup email communication with your SMTP server.

- **Admin Receives Alerts**—Receive alerts from Reporter when Warning or Critical thresholds are breached.
- **User Emails Report**—Reporter users are able to email reports to other relevant personnel in the company.

Proceed to "Connect Reporter to Email Server" on page 33.

**Manage Databases**

After you create databases and manage begin generating and managing reports (filters, emailing, and so on), you might find a need to modify existing configurations.

For a series of tasks, proceed to "Manage Existing Databases" on page 38.

**CLI**

Some tasks are only available through the Reporter CLI. See "Reference: CLI" on page 46.

**Other Tasks**

- Change the Reporter Interface Language on page 42
- "Change an Admin Password" on page 44
- License Reporter
Reporter 10.x Administrator Guide

- "Set Reporter Email From Value" on page 45
- Back Up and Restore CLI Configuration
- "Reference: Web API Parameter Syntax" on page 56
Connect Reporter to Email Server

To enable Reporter to send administrators alerts when system resources reach specified use levels and to allow users to email reports to others, you must establish a connection between Reporter and your SMTP server.

Specify the primary and backup SMTP servers to which Reporter connects.

**Prerequisite**

To configure these options, you must know the following.

- The IP address of the primary and backup SMTP servers.
- The authentication credentials to these servers.

**Procedure**

1. On the Administration > General Settings page, select Reporter Settings > System Settings > External Servers > Email.
a. Enter the **Primary SMTP Server** IP address or hostname.

b. Specify the **From** address used in e-mails. For example: SiteBReporter@mycompany.com. This email address displays in From field of the sent email and *must* be a valid address. You can use an existing generic IT address if you have one or add a new address to your email database.

c. If they are required by the server, enter the SMTP server access credentials.

d. (Optional) Enter the information for a backup SMTP server if available.

2. Click **Save**.
Email Alerts to Administrator

Configure Reporter to send an alert e-mail to specified recipients when report processing breaches a system resource threshold setting. Reporter monitors the following resources:

- Disk Storage: The current amount of filled disk space (GBs) and total capacity on the system.
- Physical Memory: The current amount of GBs used by physical memory, the percent used, and total capacity of the Reporter process.

Use this data to adjust system resources. For example, if the same system consistently sends disk space alert messages, reconsider your Reporter sizing requirements.

**Prerequisite**

Configure Reporter to connect to one of your enterprise’s SMTP (mail) servers. See "Connect Reporter to Email Server" on page 33.

**Procedure**

2. Specify who receives the alerts. Show screen...

![Alerts: Specify email alerts](image)

   a. Enter the e-mail addresses of the alert recipients. Typically, this is an IT member who is responsible for managing Reporter and/or network efficiency.

   b. By default, Reporter sends notifications when either the **Warning** or **Critical** thresholds are breached. You have the option to clear one or both (clear both prevents any notification).

   c. (Optional, recommended) To verify that Reporter sends notifications to the correct addresses, click Test Alert Email.

   d. After you verify that the recipients received the test message, click Save.
Monitor Reporter Operations

Reporter provides features that enable you to monitor events and current operations.

The following information describes links on the Administration > System Overview > Reporter System Information left-side menu. In some cases, you are able to perform executive actions.

View Current Reporter System Overview

The System Diagnostics link provides several metrics. If you are in communication with Blue Coat Technical Support, you might be asked to provide information that Reporter displays in this area.

System Overview

- **Reporter Version**—The current version of Reporter that is installed on the appliance or VA.
- **Number of CPUs**—The number of CPUs honored by Reporter.
- **SSL**—By default, Reporter is accessed over a secure connection and this setting is enable.
- **Operating System**—The current operating system that is currently running on the Reporter system.
- **Web Server Port**—By default, the Reporter access URL requires port number 8082. For example: https://192.168.0.1:8082.
- **Current Log Lines**—The total number of log lines in loaded databases.

The Licensing Information area provides the state and expiration date of the current license.

VA version—Reporter monitors the system resource configurations against the specifications in the installed license. If Reporter detects significant differences between them, it generates an alert event indicating the appliance is running with an unsupported license configuration.

For the Upload Diagnostics feature, see "Diagnose Reporter" on page 68.

System Resources

This area displays how much system resource that Reporter is currently consuming. This includes physical memory. If the Used levels consistently approach the Capacity levels, re-evaluate your sizing requirements.

Database Overview

This area provides a table of database and log processing statistics. The History links provide much more granular information.

View Current Users and Active Reports

The Active Users/Reports link provides the following information.

- **Active Users**—Who is logged into this Reporter instance right now, including details such as access privilege (admin or user) and log in time. If you do not recognize a user access, you have to option to select Actions > Force User Logout and investigate.
- **Active Reports**—Provides all of the metrics for a given report that is active right now, including the log source and database used to generate the report; the output type (such as PDF); the accessing user and their role; and the current report state. You might need to perform a maintenance task that cannot wait for off-peak hours, which might require the halt report **Action**. This information allows you to notify the users.

**View the System Event Log**

The **System Event Log** is a record of all Reporter transactions, which can assist you with troubleshooting. See Diagnose Reporter on page 68.

**View User-Initiated Information**

**View Archived Reports**

Reporter users can archive (save) a report on the Reporter instance. They might do this to ensure the report remains accessible while an investigation occurs. An admin has the ability to remove these reports. For example, the local disk storage requires more space and some reports are from a lengthy amount of time ago. The page provides the report owner information for contacting.

**View Scheduled Tasks**

Reporter users can schedule various report tasks, such as setting specific generation times. The **Scheduled Tasks** page displays pending tasks. This page also displays failed tasks, which allows you to monitor task efficiency. The **Run Status** field indicates upcoming scheduled tasks (**Not Run**). If the status is **Failed**, there was a problem with the report generation task. Notify the person listed in the **User** field so they can investigate and re-configure the task. You also have the ability to alter tasks. For example, an employee who schedules Reporter tasks might no longer be with the company.
Manage Existing Databases

After you create databases and assign log sources, you might have a requirement to alter database parameters, change default values, halt processing actions, or delete obsolete databases.

**Expire Now**

This feature allows you to purge the database based on the number of log lines. You can also perform this task on demand as this task does not need to be scheduled. However, you can set a custom purge limit.

1. Select General Settings > Reporter Settings > Data Settings > Databases.
2. In the row of the database to change, select Expire Database from the drop-down list in the Actions column.
3. Set the amount of log lines to expire and click Expire Now.

**Unload a Database to Conserve Resources**

Unloading the database takes it offline. You might encounter a scenario where a database is not currently necessary, but you are not ready to completely remove it from the system because it might be required at a later time. You cannot view reports for this database (and scheduled events for that database will not run) while it is unloaded.

1. Select General Settings > Reporter Settings > Data Settings > Databases.
2. In the row of the database to change, select Unload Database from the drop-down list in the Actions column.
3. The Status column changes from Loaded to Unloaded (depending on the size of the database, this process might require several minutes to complete).
4. To reload the database, repeat the procedure and select Load Database (if the database is currently unloading, this option is not available).

**Change Database and Log Source Parameters**

When you created databases and assigned log file sources, you followed steps in a wizard. For any database, you can access each of those wizard pages individually and change a parameter.

**Database**

- Database name
- Log sources
- Database data expiration

1. Select General Settings > Reporter Settings > Data Settings > Databases.
2. In the row of the database to change, select the drop-down list in the Actions column.
3. Select an option to change.
   - Set Name — Change the name of the database.
   - Set Log Sources — Add or delete the location of folders that feed log data into the database.
- Set **Expiration** – Change the expiration time frame of access log data.

4. Change the parameter.

5. Click **Save**.

![Clicking Reset reverts the parameters to their previously saved values.]

**Log Source**

- Description (name)
- Folder location
- Post-processing actions

![Changing log source options requires halting the log source processing.]

1. Select **General Settings > Reporter Settings > Data Settings > Log Sources**.

2. You cannot change log source parameters while the log source is operating. In the row of the log source to change, select the drop-down list in the Actions column.

   Select **Stop Log Source**. Notice that the status column displays unloaded. If the log source is processing a log file when you select **Stop Log Source** or unload its database, it immediately stops processing the current log file. If you later reload the database or restart the log source, the log source locates the unfinished log file and completes its processing first, then resumes normal operation.

3. Re-select the drop-down list in the **Actions** column and select an option to change.
   
   - **Set Description**—Change the description of the log source.
   
   - **Set Location for Local/FTP File Source**—Change the location of this specific log source.
   
   - **Set Processing Action**—Change what happens to log files after Reporter processes them.

4. Click **Save**.

![Clicking Reset reverts the parameters to their previously saved values.]

5. Select the drop-down list in the **Actions** column again and select **Start Log Source**. Reporter begins processing logs from the new or additional locations.

**Match Access Log Formats for Filtering**

In generated reports, the **Reports To, Self, and Live Group** filter criteria requires Reporter to match the username format used in the log files sent from the ProxySG appliance. If the formats do not match, these filters return no results.

The username format can be one of the following.

- **Login Name**—Example: ellen.ripley

- **Domain Name/Login Name**—Example: EX-LV426\ellen.ripley

- **LDAP FQDN**—Example: "cn=ellen.ripley,ou=users,dc=bravo,dc=examplecorp,dc=com"
Login Name is the default ProxySG appliance access log and Reporter setting. If the ProxySG username format differs from the Reporter configuration, perform the following steps.

1. Select General Settings > Reporter Settings > Data Settings > Databases.
2. In the row of the database to change, select Actions > Other Options.
3. In the Username Log Settings area, select the matching format.
4. Click Save.

Change Cost Calculators

Some reports display data that estimates how much user browsing activity translates to costs. By default, Reporter estimates the costs at .1 United States dollar per MB and 20 United States dollars per hour. If you do not believe that these values accurately represent your enterprise costs, you can change the calculation rates. For localization, you can also change the type of currency.

1. Select General Settings > Reporter Settings > Data Settings > Databases.
2. In the row of the database to change, select Actions > Other Options.
3. In the Cost Calculation area, enter new value.
a. From the Currency drop-down list, select the monetary value for your country.

b. **Cost per MB** field—Reporter uses this value to calculate the cost based on the amount of downloaded content by each user.

c. **Cost per Hour** field—Reporter uses this value and estimated user browse time to calculate how much money each user cost the company.

4. Click **Save**.

Clicking **Reset** reverts the values to their previously saved values.

### Change Default Report Row Limits

Reporter enables users to e-mail reports to others, download reports to local systems, and store archived versions on the Reporter server. In some enterprises, access log databases can grow very large, which means performing any of the aforementioned actions can clog exceed system capabilities and storage capacities. You can impose limits on how much of a report is sent or stored.

1. Select **General Settings > Reporter Settings > Data Settings > Databases**.
2. In the row of the database to change, select **Actions > Other Options**.
3. In the **Report Generation Limits** area, enter new value.

![Set Other Options for myDB](image)

4. Click **Save**.

| Clearing an option removes the limit for that parameter; do so with caution and understanding of resource impact. |
Change the Reporter Interface Language

If your access log data was generated in a supported language, you can change the language of the Reporter Management Console.

Support Languages

- Chinese (Simple and Traditional)
- English (UK)
- English (US)
- French
- Japanese

How Do I?

You must change the language before logging in (you can log out and change the language at any time). The list is located on the bottom-right corner of the log in screen.
**Convert International Domain Names**

An Internationalized Domain Name (IDM) is one that contains non-ASCII characters; for example, Asian-language characters. If the Access Logs contains this type of data, you can configure Reporter to convert this characters to Punycode.

1. On the Administration > General Settings page, select System Settings > Server Settings.
2. In the Report Generation area, select Enable Internationalized Domain Names.
3. Click Save.
Any Reporter Admin can change their access password.

**Notes**

- You are not allowed to change your password if you accessed Reporter using your LDAP access credentials. If you are unsure about this, contact your network security IT representative.
- The initial Reporter admin has the ability to remove other admin users.

**Procedure**

1. On the Administration > General Settings page, select Personal Settings > Change Password.
2. Enter your initial password, followed by your new password twice.
3. Click Save.
Set Reporter Email From Value

Reporter enables you to email generated reports to other people. The first time you perform this action, the email address you enter in the From address becomes your default Reporter e-mail address. You can change it on a per-report e-mailing action basis without changing the default, or you can change the default.

1. On the Administration > General Settings page, select Personal Settings > Email.
2. Enter the new e-mail address.
3. Click Save.
The Reporter CLI provides a set commands that allows you to manage and change networking settings (IP, Mask, Gateway, DNS), configure / change username / password, and generate SSL self-signed certificate.

---MENU---
1) Command Line Interface
2) Setup
---MENU---

Enter option:

Option 2 begins the guided setup, as described in Install Reporter on a Virtual Appliance.

Option 1 enters basic CLI mode.

### Basic Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enter privileged command mode. See enable mode commands in next section.</td>
</tr>
<tr>
<td>exit</td>
<td>Exit the CLI/mode.</td>
</tr>
<tr>
<td>help (or ?)</td>
<td>Displays help.</td>
</tr>
<tr>
<td>ping</td>
<td>Ping utility.</td>
</tr>
<tr>
<td>show</td>
<td>Show the subordinate command structure/options.</td>
</tr>
<tr>
<td>tracepath</td>
<td>Trace path utility.</td>
</tr>
</tbody>
</table>

### Enable Mode Commands

Reporter> enable

<table>
<thead>
<tr>
<th>Command</th>
<th>Sub-Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>IMPORTANT: This command does not back up databases or configuration. At this time, Blue Coat does not have a use case for this command, but functionality might be available in future releases.</td>
<td></td>
</tr>
<tr>
<td>create</td>
<td>Creates a backup of a small subset of configurations set in the CLI.</td>
<td></td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a backup.</td>
<td></td>
</tr>
<tr>
<td>export</td>
<td>Exports a backup to a local server.</td>
<td></td>
</tr>
<tr>
<td>import</td>
<td>Imports a backup from a local server.</td>
<td></td>
</tr>
<tr>
<td>restore</td>
<td>Restores a backup.</td>
<td></td>
</tr>
<tr>
<td>view</td>
<td>View available backups.</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td>Turn off privileged commands.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exit current CLI mode.</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Sub-Commands</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>http-proxy</td>
<td>configure</td>
<td>Modifies the explicit HTTP proxy configuration.</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Disables use of explicit HTTP proxy configuration.</td>
</tr>
<tr>
<td></td>
<td>enable</td>
<td>Enables use of explicit HTTP proxy configuration.</td>
</tr>
<tr>
<td>installed-</td>
<td>add</td>
<td>Downloads and installs a new system image.</td>
</tr>
<tr>
<td>systems</td>
<td>default</td>
<td>Sets the default system image.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Deletes a system image.</td>
</tr>
<tr>
<td></td>
<td>lock</td>
<td>Locks a system image.</td>
</tr>
<tr>
<td></td>
<td>unlock</td>
<td>Unlocks a system image.</td>
</tr>
<tr>
<td></td>
<td>view</td>
<td>View the list of installed system images.</td>
</tr>
<tr>
<td></td>
<td>view-downloads</td>
<td>View the progress of systems being downloaded and installed.</td>
</tr>
<tr>
<td>license</td>
<td>download</td>
<td>Updates license from Blue Coat server.</td>
</tr>
<tr>
<td></td>
<td>download-from url</td>
<td>Download license from server at specified URL.</td>
</tr>
<tr>
<td></td>
<td>view</td>
<td>View license information and status of the last license download.</td>
</tr>
<tr>
<td>ping</td>
<td>status</td>
<td>Ping utility.</td>
</tr>
<tr>
<td>raid</td>
<td>status</td>
<td>View the current RAID array status. This output assists with troubleshooting drive issues.</td>
</tr>
<tr>
<td>restart</td>
<td>reboot</td>
<td>Reboots the appliance.</td>
</tr>
<tr>
<td></td>
<td>graceful</td>
<td>Allows Reporter to unload its databases and stop all log processing before terminating the process and restarting the appliance.</td>
</tr>
<tr>
<td></td>
<td>forceful</td>
<td>Reboots the appliance but does not unload databases or stop processing beforehand. Use with caution, as this might result in database corruption. Considered a last resort method.</td>
</tr>
<tr>
<td>restore-</td>
<td>factory-defaults</td>
<td>Restores the system to factory defaults and reboot.</td>
</tr>
<tr>
<td>defaults</td>
<td>factory-defaults-halt</td>
<td>Restores the system to factory defaults and halt.</td>
</tr>
<tr>
<td></td>
<td>factory-defaults-shutdown</td>
<td>Restores the system to factory defaults and shutdown.</td>
</tr>
<tr>
<td>security</td>
<td>enable-password</td>
<td>Enables password for enable commands.</td>
</tr>
<tr>
<td></td>
<td>generate-ssl-certificate</td>
<td>Generate a default self-signed SSL Certificate. For scenario information, see Diagnose Reporter on page 68.</td>
</tr>
<tr>
<td></td>
<td>password</td>
<td>Specifies console account password.</td>
</tr>
<tr>
<td></td>
<td>unset-enable-password</td>
<td>Disables password for enable commands.</td>
</tr>
<tr>
<td>service</td>
<td>disable-verbose-logging</td>
<td>Disables verbose logging.</td>
</tr>
<tr>
<td></td>
<td>enable-verbose-logging</td>
<td>Enables verbose logging to assist with troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>upload-diagnostics</td>
<td>Uploads diagnostic information to Blue Coat or local server.</td>
</tr>
<tr>
<td>Command</td>
<td>Sub-Commands</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show</td>
<td>http-proxy</td>
<td>Shows HTTP proxy status and configuration.</td>
</tr>
<tr>
<td></td>
<td>installed-systems</td>
<td>View the list of installed system images.</td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td>Shows interface status and configuration.</td>
</tr>
<tr>
<td></td>
<td>license</td>
<td>View license information and status of the last license download.</td>
</tr>
<tr>
<td></td>
<td>setupinfo</td>
<td>Shows system configuration.</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>View SNMP settings.</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>Shows system status.</td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>Displays the system version.</td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
<td>Shuts the system down.</td>
</tr>
<tr>
<td></td>
<td>graceful</td>
<td>Allows Reporter to unload its databases and stop all log processing before terminating the process and powering down the appliance.</td>
</tr>
<tr>
<td></td>
<td>forceful</td>
<td>Powers down the appliance but does not unload databases or stop processing beforehand. Use with caution, as this might result in database corruption. Considered a last resort method.</td>
</tr>
<tr>
<td>snmp</td>
<td>disable-remote-read-access</td>
<td>Disallows remote read access.</td>
</tr>
<tr>
<td></td>
<td>enable-remote-read-access</td>
<td>Allows read-only remote access.</td>
</tr>
<tr>
<td></td>
<td>set-community</td>
<td>Sets the community string.</td>
</tr>
<tr>
<td></td>
<td>view</td>
<td>View SNMP settings.</td>
</tr>
<tr>
<td>tracepath</td>
<td></td>
<td>Trace path utility.</td>
</tr>
<tr>
<td>verify-hardware</td>
<td></td>
<td>Verifies the hardware configuration.</td>
</tr>
</tbody>
</table>
Reference: Log Fields

This section provides a reference table that lists the report field to log field association. Report fields are what comprise various reports, based on the information contained in the access log. The contents of an access log are determined by the log field names (which determine what data types are captured during the ProxySG appliance logging process). Some log field names correlate to absolute data (such as URLs), others derive information from access log variables (such as browsing duration).

Log Field Best Practices

Certain access log fields are critical to proper Reporter operation. To prevent Reporter from disregarding some log lines, the databases require the following fields.

- cs-host, cs-uri-host, or cs-uri-hostname
- sc-status
- cs-uri-scheme
- c-ip, x-client-ip, x-client-address, c-dns or x-cs-username-or-ip
- rs(Content-Type)
- sc-filter-result or x-exception-id
- x-virus-id

For the Page View Combiner (PVC) to operate correctly, Reporter requires the following additional fields.

See About the Page View Combiner on page 15.

- cs(Referer) or x-cs(Referer)-uri
- x-exception-id or sc-filter-result (x-exception-id preferred)
- sc-filter-category, cs-category, or cs-categories

For the PVC to operate correctly for video reports, Reporter requires the following additional fields.

- cs-host, cs-uri-host, or cs-uri-hostname
- cs-uri-scheme
- c-ip, x-client-ip, x-client-address or c-dns, x-cs-username-or-ip
- sc-status
- sc-filter-result or x-exception-id
- x-virus-id
- cs-method
- time-taken
To properly populate all default Dashboard reports, Reporter requires the following fields in addition to those above.
- cs-uri-scheme
- s-session-id

To populate all default video reports, Reporter requires the following fields.
- cs-host, cs-uri-host, or cs-uri-hostname
- c-ip, x-client-ip, x-client-address, c-dns, or x-xs-uri-username-or-ip
- x-cache-info
- cs-auth-group or cs-auth-groups
- x-rs-streaming-content

**Main Log Field Names**

The following table provides what log field provides data for what report field. *Italicized* report field text indicates that the resulting data is *derived* (sometimes combined with data from other fields).

<table>
<thead>
<tr>
<th>Report Field Name</th>
<th>Log Field Name</th>
<th>Report Field Name</th>
<th>Log Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs(Referer)</td>
<td>cs(Referer)</td>
<td>browse_time</td>
<td><em>Calculated at run-time from user session and stored as database field.</em></td>
</tr>
<tr>
<td>c_ip</td>
<td>c-ip</td>
<td>cs_auth_group</td>
<td></td>
</tr>
<tr>
<td>cs_bytes</td>
<td>cs-bytes</td>
<td>cs_host</td>
<td>cs-host</td>
</tr>
<tr>
<td>cs_method</td>
<td>cs-method</td>
<td>cs_uri_extension</td>
<td>cs-uri-extension</td>
</tr>
<tr>
<td>cs_uri_path</td>
<td>cs-uri-path</td>
<td>cs_url_query</td>
<td>cs-url-query</td>
</tr>
<tr>
<td>cs_url_scheme</td>
<td>cs-url-scheme</td>
<td>cs_user_agent</td>
<td>cs(User-Agent)</td>
</tr>
<tr>
<td>cs_username</td>
<td>cs-username</td>
<td>date</td>
<td></td>
</tr>
<tr>
<td>date_time</td>
<td>date + time</td>
<td>day_of_week</td>
<td><em>Derived from date.</em></td>
</tr>
<tr>
<td>hour_of_day</td>
<td>Derived from time.</td>
<td>month</td>
<td><em>Derived from date.</em></td>
</tr>
</tbody>
</table>
### Reports/Log Fields Matrix

This section provides a table that lists which main-format access log fields are required to populate each pre-defined report in the **User Behavior**, **Security**, and **Bandwidth Usage** groups on the **Reports** tab. Use this reference to understand how log fields relate to report data and aid in your customization of reports.

<table>
<thead>
<tr>
<th>Report Field Name</th>
<th>Log Field Name</th>
<th>Report Field Name</th>
<th>Log Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>requests (same as page views or hits)</td>
<td>Calculated during database generation and stored as database field.</td>
<td>rs_content_type</td>
<td>rs(Content-Type)</td>
</tr>
<tr>
<td>s_action</td>
<td>sc-bytes</td>
<td>sc_filter_category</td>
<td>cs-categories (or cs-category or sc-filter-category)</td>
</tr>
<tr>
<td>sc_status</td>
<td>sc-status</td>
<td>time</td>
<td>time</td>
</tr>
<tr>
<td>total_bytes</td>
<td>cs-bytes + sc-bytes</td>
<td>url</td>
<td>Combined from (uri-scheme://cs-host/cs-url-path [cs-url-query]).</td>
</tr>
<tr>
<td>verdict</td>
<td>x-exception-id(sc-filter-result if x-exception-id is not present).</td>
<td>week</td>
<td>Derived from date.</td>
</tr>
<tr>
<td>x_virus_id</td>
<td>x-virus-id</td>
<td>year</td>
<td>Derived from date.</td>
</tr>
</tbody>
</table>

### Main Log Required Field Matrix

These reports are URL-centric; they display reports that reflect browsing activity.
<table>
<thead>
<tr>
<th>Report Group</th>
<th>Report Name</th>
<th>Required Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Behavior</td>
<td>Blocked Web Browsing per User</td>
<td>sc-filter-result, cs-username, cs-bytes, sc-bytes</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Category</td>
<td>{cs-categories -or- sc-filter-category}, cs-bytes, sc-bytes</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Day</td>
<td>date, sc-bytes, cs-bytes</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Day of Week</td>
<td>date, cs-bytes, sc-bytes, time, time-taken</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Group</td>
<td>cs-auth-group, cs-bytes, sc-bytes</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Hour of Day</td>
<td>time, cs-bytes, sc-bytes, time-taken</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Month</td>
<td>date, cs-bytes, sc-bytes, time, time-taken</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per Site</td>
<td>cs-host, {cs-categories -or- sc-filter-category}, cs-bytes, sc-bytes, time_taken</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per User</td>
<td>cs-username, cs-bytes, sc-bytes</td>
</tr>
<tr>
<td></td>
<td>Web Browsing per User and Category</td>
<td>cs-username, sc-filter-category or cs-categories, sc-bytes, cs-bytes</td>
</tr>
<tr>
<td></td>
<td>Web Searches</td>
<td>cs-uri-query (Also requires Blue Coat Web Filter (BCWF) enabled.)</td>
</tr>
<tr>
<td>Report Group</td>
<td>Report Name</td>
<td>Required Fields</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security</td>
<td>Blocked Web Browsing by User Agent</td>
<td>sc-filter-result, cs(User-Agent), cs-bytes, sc-bytes</td>
</tr>
<tr>
<td></td>
<td>Blocked Web Sites</td>
<td>sc-filter-result, cs-host, {sc-filter-category -or- cs-categories}, cs-bytes, sc-bytes</td>
</tr>
<tr>
<td></td>
<td>Filtering Verdict Trend by Day</td>
<td>date, sc-filter-result</td>
</tr>
<tr>
<td></td>
<td>Malware Requests Blocked by Site</td>
<td>cs-bytes, cs-host, sc-bytes, sc-filter-category, time-taken</td>
</tr>
<tr>
<td></td>
<td>Potential Malware Infected Clients</td>
<td>c-ip, cs-bytes, cs-host, sc-bytes, sc-filter-category, time-taken</td>
</tr>
<tr>
<td></td>
<td>Potential Threats</td>
<td>x-virus-id, sc-filter-category</td>
</tr>
<tr>
<td></td>
<td>ProxyAV Malware Detected: Client IP</td>
<td>c-ip, cs-bytes, sc-bytes, time-taken, x-virus-id</td>
</tr>
<tr>
<td></td>
<td>ProxyAV Malware Detected: Names</td>
<td>cs-bytes, sc-bytes, time-taken, x-virus-id</td>
</tr>
<tr>
<td></td>
<td>ProxyAV Malware Detected: Sites</td>
<td>cs-bytes, cs-uri-path, cs-uri-query, cs-uri-scheme, sc_bytes, time-taken, x-virus-id</td>
</tr>
<tr>
<td></td>
<td>Risk Groups</td>
<td>sc-filter-category</td>
</tr>
<tr>
<td></td>
<td>SSL Certificate Categories</td>
<td>{cs-username -or- c-ip}, s-action, x-rs-certificate-hostname, sc-bytes, cs-uri-port</td>
</tr>
<tr>
<td></td>
<td>SSL Certificate Errors</td>
<td>x-rs-certificate-observed-errors, x-rs-certificate-hostname, sc-bytes, cs-uri-port</td>
</tr>
<tr>
<td></td>
<td>Trend of Potential Threats</td>
<td>x-virus-id, sc-filter-category</td>
</tr>
</tbody>
</table>
## Web Application Reports

<table>
<thead>
<tr>
<th>Report Field Name</th>
<th>Required Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application Name</td>
<td>x-bluecoat-application-name, hits, page-views, browse-time, cost-time, total-</td>
</tr>
<tr>
<td></td>
<td>bytes, cost-bytes, sc-bytes, cs-bytes, cache-bytes, rs-bytes</td>
</tr>
<tr>
<td>Web Application Operation</td>
<td>x-bluecoat-application-operation, hits, page-views, browse-time, cost-time,</td>
</tr>
<tr>
<td></td>
<td>total-bytes, cost-bytes, sc-bytes, cs-bytes, cache-bytes, rs-bytes</td>
</tr>
<tr>
<td>Web Application Detailed Report</td>
<td>x-bluecoat-application-name, x-bluecoat-application-operation, c-ip, total-</td>
</tr>
<tr>
<td></td>
<td>bytes, cost-bytes, hits, sc-bytes, cs-bytes, page-views, browse-time, cost-time,</td>
</tr>
<tr>
<td></td>
<td>cache-bytes</td>
</tr>
<tr>
<td>Web Browsing per Web Application Name</td>
<td>x-bluecoat-application-name, c-ip, total-bytes, cost-bytes, sc-bytes, cs-</td>
</tr>
<tr>
<td>and Client IP</td>
<td>bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
<tr>
<td>Web Browsing per Web Application Name</td>
<td>x-bluecoat-application-name, cs-user-name, total-bytes, cost-bytes, sc-bytes,</td>
</tr>
<tr>
<td>and User</td>
<td>cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
</tbody>
</table>

## Video Usage Reports
<table>
<thead>
<tr>
<th>Report Field Name</th>
<th>Required Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP Video</td>
<td>c-ip, total-bytes, cost-bytes, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
<tr>
<td>Flash Streaming Bandwidth Cost per Day</td>
<td>date, page-views, browse-time, sc-bytes, rs-bytes, total-bytes, cs-bytes, cache-bytes</td>
</tr>
<tr>
<td>Group Video</td>
<td>cs-auth-group, total-bytes, cost-bytes, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
<tr>
<td>Video Application Delivery Method</td>
<td>x-rs-streaming-content, total-bytes, cost-bytes, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
<tr>
<td>Video Application Type</td>
<td>x-cache-info, total-bytes, cost-bytes, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
<tr>
<td>Video Applications</td>
<td>x-rs-streaming-content, cs-host, total-bytes, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
<tr>
<td>Video Page Detail</td>
<td>cs-host, filename, c-ip, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes, total-bytes</td>
</tr>
<tr>
<td>Video Site</td>
<td>cs-host, total-bytes, sc-bytes, cs-bytes, hits, page-views, browse-time, cost-time, cache-bytes</td>
</tr>
</tbody>
</table>
Reference: Web API Parameter Syntax

The following reference sections describe all parameters to each Web API endpoint. As a general rule, complex parameter values are pipe (|) separated lists; for example: abc|def|123.

Common Parameters

The following parameters are used by all HTTP endpoints (create, cancel, status, and download).

Parameter: username

Description

The same username that could be used to login to the Reporter user interface. Just like the web interface, the Web API enforces access control based on identity and roles. Also like the web interface, the Web API supports both local users and LDAP users.

Example

username=bcrepuser

Parameter: password

Description

The same password that could be used to login to the Reporter user interface.

Example

password=bluepass

Parameter: reportId

Description

The reportId that is contained in the response to the /webapi/create request. This parameter is required for all requests except the /webapi/create request.

Example

reportId=14329

Parameter: responseFormat

Description

The HTTP response type (not the output format of the report). Valid values are xml, html, and plain (the default). The response format applies to the create, cancel, and status endpoints (not to download).
Example 1

Request:
```plaintext
responseFormat=plain
```
Response:
```plaintext
reportId:5111890
state:2
percent_done:97
user:user_admin
role:_admin
reportName:Date_Data_12
database:database_5a541ee0aa0e11debf01f18168b313eb
```

Example 2

Request:
```plaintext
responseFormat=xml
```
Response:
```xml
<result>
  <reportId>327774</reportId>
  <reportName>test adf asdf</reportName>
  <state>2</state>
  <percentDone>0</percentDone>
  <user>user_9d2f2430aa0e11debf01f18168b313eb</user>
  <role>role_866df230aa0e11debf01f18168b313eb</role>
  <database>database_42587110aa0e11debf01f18168b313eb</database>
</result>
```

**End Point: /api/create**

Creates a new report definition and begins generation of the report.

**Required Parameters**
- username
- password
- database
- role
- label
- summarizeBy and/or columns (must have summarizeBy, columns, or both)

**Optional Parameters**
- format
- sort
- action
- filter
- graphType
- graphColumns
- dateStart
- dateEnd
- dateRelativeUnit
- emailTo
- emailCC
- emailBCC
- emailSubject
- emailBody

**Example—One-level summary report; archived to server**

https://localhost:8082/api/create?
username=test&
password=test&
database=mydb&
role=myrole&
label=myreport1&
summarizeBy=sc_filter_category

**Example—Two-level summary report; sorted, filtered, and archived to server**

https://localhost:8082/api/create?
username=test&
password=test&
database=mydb&
role=myrole&
label=myreport2&
summarizeBy=sc_filter_category | c_ip
columns=hits|page_views&
sort=c_ip:desc&
filter0=sc_filter_category|IS|Adult/Mature%20Content|Alcohol/Tobacco&action=download

**Parameter: database**

**Description**

Reporter database for report.

**Example**

database=secdb1
Parameter: role

Description
User's role that will be used for access control.

Example

role=repgenerator

Reporter administrators can use a hidden role named: _admin. This role has access to all fields and all databases and can be used as the role parameter the same as a user defined role.

Parameter: format

Description
The output format of the generated report. Valid values are csv, pdf, or json.

Example

format=pdf

The default is pdf.

Parameter: label

Description
Report name.

Example

label=bobreport

Parameter: summarizeBy

Description
List of database fields that provide summary information (similar to SQL GROUP BY). Reports can have up to three summarizeBy fields. If there are no summarizeBy fields, the report is a Full Log Detail report.

Value Syntax

summarizeBy=option

Examples

One-level report

summarizeBy=c_ip

Two-level report

summarizeBy=cs_username|c_ip
Three-level report
   summarizeBy=cs_username|c_ip|cs_host
Two-level report with maximum of five and ten rows respectively for each level
   summarizeBy=cs_username|cs_host&rows=5|10

Parameter: columns

Description
List of database fields to display (in addition to the summarizeBy fields).

Examples
   columns=hits
   columns=hits|page_views

Parameter: rows

Description
Configures the number of rows returned for each level of the report. Up to three values can be configured (for three-level summary reports). Values are pipe (|) separated.

Examples
   rows=1000
   rows=10|10|10

Parameter: sort

Description
Field name that Reporter uses to sort the data. Only one field is allowed.

Examples
   sort=hits
If specified, the default is to sort by order of summarizeBy fields.

Parameter: action

Description
Action to perform with the generated report. Valid actions are archive, email, and download. The email and archive actions are the most simple to use. A single HTTP request to /webapi/create generates the report and performs the specified action. Downloading a report is more complicated and requires a sequence of requests to generate the report, verify the report is complete, and download the result. Downloading is discussed in a later section. The default action is archive.
Examples

action=email

If the action is email, the emailTo parameter is also required; other parameters are also available. See the subsequent emailXX parameters.

Parameter: emailTo

Description

This parameter is required if the action is specified as email. It specifies the primary recipient(s) of the report in RFC822 format.

Examples

emailTo=rptadmin@example.com

Parameter: emailCC

Description

This parameter is required if the action is specified as email. It specifies the carbon copy (CC) recipient(s) of the report in RFC822 format.

Example

emailCC=ITwatchlist@example.com

Parameter: emailBCC

Description

This parameter is required if the action is specified as email. It specifies the blind carbon copy (BCC) recipient(s) of the report in RFC822 format.

Examples

emailCC=ITwatchlist@example.com

Parameter: emailSubject

Description

This parameter is only relevant if the action is email. It specifies the text to be included in the email subject line.

Example

emailSubject=Monday+web+use+reports

To be properly processed by command shells, the API might require plus signs (+) instead of spaces.

Parameter: emailBody
**Description**

This parameter is only relevant if the action is email. specifies the text to be included in the email message body.

**Examples**

```
emailBody=This+report+provides+weekly+web+use+data+for+the+
west+coast+office
```

*To be properly processed by command shells, the API might require plus signs (+) instead of spaces.*

**Parameter: filterN**

**Description**

Reports can contain multiple filters (analogous to the WHERE clause of a SQL query). Each filter is composed of three components separated by a pipe (|) character: field, operator, and values. If a report includes multiple filter parameters, the filters are anded together. However, if a single filter contains multiple values, the values are ored together. By default, no filters are applied.

**Examples**

```
filter0=sc_filter_category|IS|*spyware*|*suspicious*
```

**Parameter: graphType**

**Description**

The type of graph to be rendered into the report. This parameter is only applicable when format=pdf. Graphs are currently not supported for two and three-level reports. The valid graph types are Pie, Column, Line, Area, Scatter, Bar, and Stack-bar.

**Examples**

```
graphType=Pie
```

*If graphType is specified, you must also specify graphColumns. The default is no graph or report.*

**Parameter: graphColumns**

**Description**

Indices of the columns to be graphed.

**Examples**

```
graphColumns=1
graphColumns=1|2|3
```

*If graphType is specified, you must also specify graphType. The default is no graph or report.*

**Parameter: dateRelativeUnit**
Description

Allows specifying a date filter using relative dates instead of an absolute start and end time. Valid values are hour, date, week, month, and year. If dateRelativeUnit is set, dateStart and dateEnd must be the number of relative units (not Unix time or an ISO 8601 string).

Examples

- dateRelativeUnit=week&dateStart=0 // Current week
- dateRelativeUnit=week&dateStart=5&dateEnd=0 // Previous 5 weeks (does not include current week)
- dateRelativeUnit=week&dateStart=5 // Previous 5 weeks (includes current week)

Parameter: dateStart

Description

Configures a beginning date filter. There are three different syntaxes for the date:

- Unix Time (number of seconds since January 1, 1970 UTC)
- ISO 8601 formatted string (for example: 2016-12-31T13:00:00-00:00).
- If dateRelativeUnit is set, it is the number of those units relative to the current time (for example: 5).
- Default—The beginning date is that of the oldest data.

Examples

- dateStart=2007-12-31T13:00:00-00:00
- dateStart=1254299093
- dateStart=5

Parameter: dateEnd

Description

Configures an ending date filter. There are three different syntaxes for the date:

- Default—The end date is that of the newest data.

Examples

- dateEnd=2007-12-31T13:00:00-00:00
- dateEnd=1254299093
- dateEnd=5

Parameter: showLast

Description

Only applicable for trend reports (must be summarized by date field); true or false.
End Point: /api/status

Checks the status of a report. Returns the running time and the percent complete.

Required Parameters

- username
- password
- reportId

End Point: /api/cancel

Cancels a running report.

Required Parameters

- username
- password
- reportId

End Point: /api/download

Downloads the report. Only valid if action=download during the create request. The response is the generated report (CSV, PDF, or JSON).

Required Parameters

- username
- password
- reportId

End Point: /api/listDatabases

Returns a list of databases that the given role can access.

Required Parameters

- username
- password
- role

End Point: /api/listFields

Returns a list of databases that the given role can access.
Required Parameters

- username
- password
- role
- database

Sample Output

Valid values for summarizeBy parameter:
============================================
year
month
week
...
Valid values for summarizeBy (in Trend Reports):
=============================================
year
month
week
...
Valid values for columns parameter (in a Summary Report):
=============================================
hits
page_views
browse_time
...
Valid values for columns parameter (in a Detail Report):
=============================================
year
month
week
...
Valid values for filter parameter:
=============================================
day_of_week
hour_of_day
c_ip
sc_status
...

Debugging

If you receive an HTTP status code of 400 to 499, it means that the request sent to Reporter was invalid. There are several reasons for invalid requests, such as invalid field, username, password, and so on. In addition to the generic status code (for example: 400), Reporter returns a more detailed error message in the body of the HTTP response that explains which part of the request is invalid and why. Some HTTP tools (such as wget) do not provide access to the response body for non-200
responses. To debug the issue, enter the URL into the browser address bar (Firefox, Internet Explorer) and press Enter. The browser displays the detailed error message. For example, the following request:

https://localhost:8082/api/create?username=test&password=test1test&database=draper&role=test&label=report1 &columns=date|url|hits|page_views|bogus

Generates the following error message:

httpStatusCode: 400
httpMessage: Bad Request
detailedMessage: Invalid column bogus

Relative Dates

When creating a report (/api/create), you can specify a date filter using absolute units or relative units. Absolute dates can be specified in Unix time or as an ISO 8601 string. Relative dates are powerful, but are slightly more complex. Relative dates specify date filters in one of the following categories: Current, Previous, and Current and Previous.

If the dateRelativeUnit parameter is set, the dateStart and dateEnd define the number of units into the past. The following are valid units: year, month, week, day, and hour.

It is important to understand that dateStart and dateEnd always represent a point in time that is on a boundary of a whole unit (year, month, week). A value of zero for dateStart or dateEnd represents the nearest whole unit in the past. Therefore, if dateStart is set to zero and dateRelativeUnit is set to year, the dateStart represents January 1, of the current year. If dateStart is set to zero and dateRelativeUnit is set to week, the dateStart represents Sunday of the current week.

Examples

In the following examples, dateRelativeUnit=year, and today's date is 2009-10-01 (YYYY-MM-DD). Thus, values for dateStart or dateEnd have the following absolute values:

0 = 2009-01-01 12:00:00 PM GMT
1 = 2008-01-01 12:00:00 PM GMT
2 = 2007-01-01 12:00:00 PM GMT
...

Current Year: (2009-01-01 - today)

dateRelativeUnit=year&dateStart=0

Previous Year (2008-01-01 to 2009-01-01)

dateRelativeUnit=year&dateStart=1&dateEnd=0

Previous Two Years (2007-01-01 to 2009-01-01)

dateRelativeUnit=year&dateStart=2&dateEnd=0

Current and Previous Year (2008-01-01 to today)

dateRelativeUnit=year&dateStart=1
Trend Reports

To create trend reports:

1. Summarize by a time based field. See "End Point: /api/listFields" on page 64 to view a list of summarizeBy fields that are usable used in trend reports.

2. Set showLast parameter to true.
Diagnose Reporter

If Reporter is experiencing a type of connection or other error, review the System Event Log. With serious problems, you might work with Blue Coat Technical Support to upload diagnostic information for analysis.

Shutdown Information (RP-S500)

Do not shut down the appliance using the switch or by removing the power cables. Abruptly removing power can result in irreparable data loss. Always use the shutdown command from the CLI to power down the appliance.

For the Reporter appliance (RP-S500), the CLI provides a command to shutdown the appliance.

```
#enable
#shutdown graceful
```

Allows Reporter to unload its databases and stop all log processing before terminating the process and powering down the appliance.

When Proxied Through a ProxySG Appliance

If the Reporter connection proxies through a ProxySG appliance that has SSL Interception enabled, you experience a certificate issue when attempting to access Reporter. You must use the browser to export the certificate and add it to the ProxySG appliance.

Symptom

Users receive a certificate error in the browser.

Scenarios

You must repeat this procedure any time a new Reporter certificate is generated, which most likely occurs from one of the following actions.

- You use the generate-ssl-certificate command to generate a new certificate (see "Reference: CLI" on page 46).
- The Reporter appliance is restored to factory defaults.

Workaround

1. Obtain the browser certificate.
   b. When Reporter displays the certificate error, click Information.
   c. Export the certificate—open it in Notepad.
   d. Copy the PEM.
2. Add to the ProxySG appliance.
a. From the ProxySG appliance Management Console, select **Configuration > SSL > Certificates**.

b. Click **Import**.

c. Paste the PEM.

d. Click **Apply**.

e. Click the **Certificate Lists** tab.

f. Add the same certificate to the **Browser Trusted List of Certificates**.

### Analyze the Reporter System Event Log

The event log is a record of all Reporter transactions. These logs are accessible on the **Admin > System Overview > Reporter System Information > System Event Log** page and reviewing them might assist you with troubleshooting.

When you select a session event log, Reporter displays the **Warnings**, **Errors**, and **Critical** levels of transaction data.

1. Select an even log session.

2. In the options header, select which details to display. In the data area, the symbols indicate to the type of journal entry.

The header displays icons, which enables you customize which types of data are displayed:

- **Info**—Not selected by default in some modes. This options toggles the most verbose event log records, as every type of Reporter transaction displays.

- **Warnings**—A light event that Reporter can often overcome by re-attempting later. For example, Reporter is not able to contact the SMTP server when attempting to send an e-mail.

- **Errors**—Errors are messages indicate something went wrong, possibly resulting in data loss. Continuing the SMTP example, Reporter reached the maximum retry attempts for a non-responsive SMTP server. That message is not sent and Reporter logs an error.

- **Critical**—Critical errors messages should be rare. They occur when a Reporter system crash is eminent. An example of this type of message is if your databases directory does not have write permissions, Reporter cannot continue and shuts down. Critical messages provide valuable information to a support person.
Upload Diagnostics to Blue Coat

If you call Blue Coat Technical Support to report a serious issue with Reporter, you might be assigned a Service Request (SR) number by the Blue Coat support person, asked to enter that number, and upload system diagnostics.

The Administration > System Overview > Reporter System Information page contains the SR Number field. When you enter the number and click Upload, Reporter sends comprehensive diagnostic data to Blue Coat for problem analysis.

If your network firewall is configured to block unproxied traffic, see the Connect to an Explicit Proxy for External Communication section in "Administrative Tasks" on page 31.

Reporter creates a .zip file named reporterdiags, which contains the diagnostic information.

If you cannot access the Reporter Management Console, you must run the bcrdiagnostics.exe application from a command line and answer the prompts.

RAID Array (RP-S500)

For the Reporter appliance (RP-S500), the CLI provides a RAID command that displays the current status of the RAID array. With this, you can view the current hard drive status.

```bash
#enable
#raid status

....
Update Time : Mon Jul 27 20:56:38 2015
State : clean
Active Devices : 24
Working Devices : 24
Failed Devices : 0
Spare Devices : 0
....
```

In the above output excerpt, the State is clean. The possible values are the following.

- Clean—RAID rebuild is completed and there are no pending writes to mirror disks.
- Clean, degraded—RAID rebuild is completed and there are no pending writes to mirror disks; however, an array contains faulty disks.
- Active, resyncing—RAID rebuild is completed and there are pending/ongoing writes to primary/mirror disks.
- Active, degraded—RAID rebuild is completed and there are pending/ongoing writes to primary/mirror disks; an array contains faulty disks.