Symantec® Reporter 10.x Reporting Guide

Product Version 10.4.1.1 — Tuesday, July 30, 2019

Copyrights

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com

Table Of Contents

Create a Database

After configuring the ProxySG appliance to upload access logs to an FTP server, you can create a Reporter database (and associated log source) that processes those access logs.

About Log Sources

Consider the following when planning how to create databases and assign log sources:

- You can configure multiple ProxySG appliances to send access logs to single directory—whether to the root directory or a subdirectory.
- No directories can be shared across multiple log sources, even if they are at the top level. This is especially important when a subdirectory is part of a tree that is owned by a different log source that has the **Process Subdirectories** option selected.
  - If no log sources are processing subdirectories, the rule is that no single directory can be shared.
  - If a subdirectory is checked by any log source, the rule is that no directories in the log source directory tree can be shared.
- Never configure a log source to process subdirectories followed by moving the processed log files into a directory that is under the top directory. This causes an endless log processing loop.
- If you configured the ProxySG appliance to upload access logs directly to the Reporter appliance, you will create a Local Log Source. A single instance of this source can only process logs from a single directory; however, you can configure the log source to process log files in any subdirectories under the configured top directory.

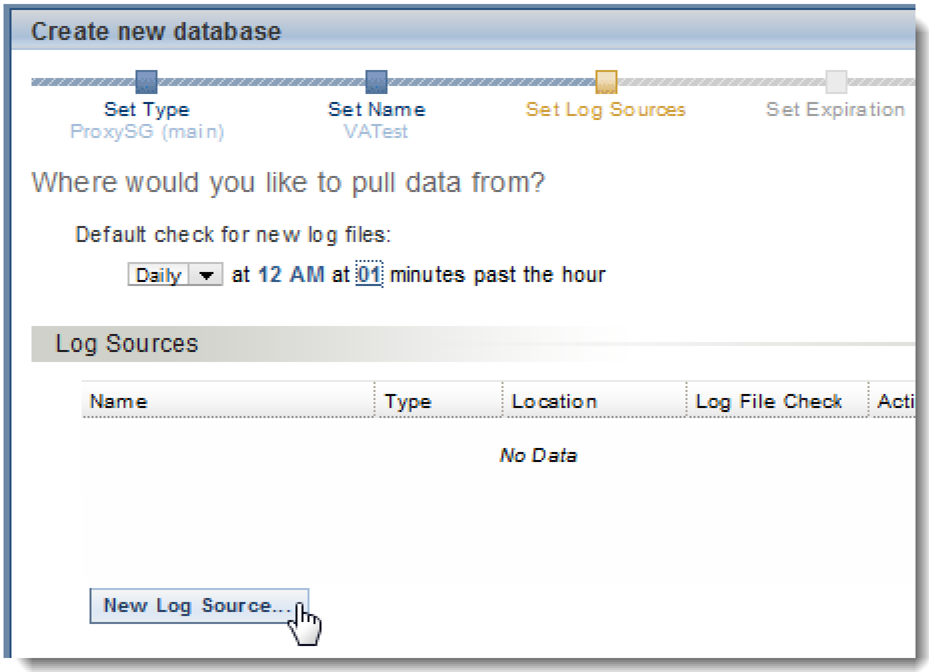
Procedure

Follow these steps to create a database that uses a ProxySG log source.

1. Access the Reporter web UI with Admin credentials.
2. Click **Administration** in the upper-right corner.
3. Select the **General Settings** tab and then **Data Settings > Databases**.
4. Create a new database.
   a. Click **New** to open the *Create New Database* wizard.
   b. **Set Type**—Accept the default **ProxySG (main)** option.

c. Select **Include Advanced Options** to configure advanced options in the next screen. Leave this box unchecked to use the default settings. (See "Create a Database" on the previous page for custom field creation.) Click **Next**.

d. **Name** the database and click **Next**.

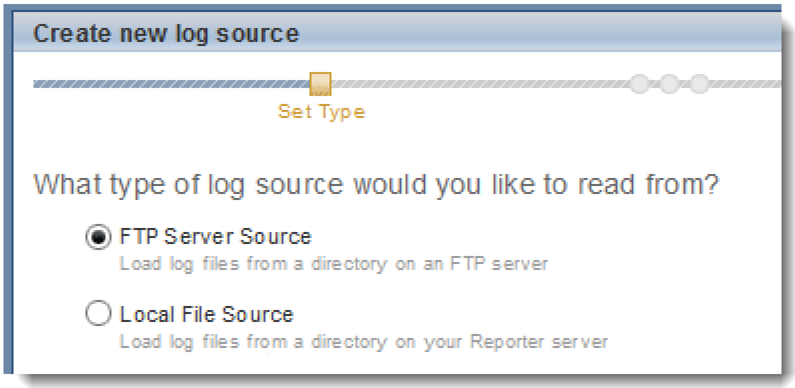


e. Set the **Default check for new log files**, or how often this database queries for yet-to-be processed access logs.

> **Note:** You can configure each **Log Source** to use this default at different times.

g. Click **New Log Source** to open the *Create New Log Source* wizard.

5. Connect to the log source.



a. Select one of the following:

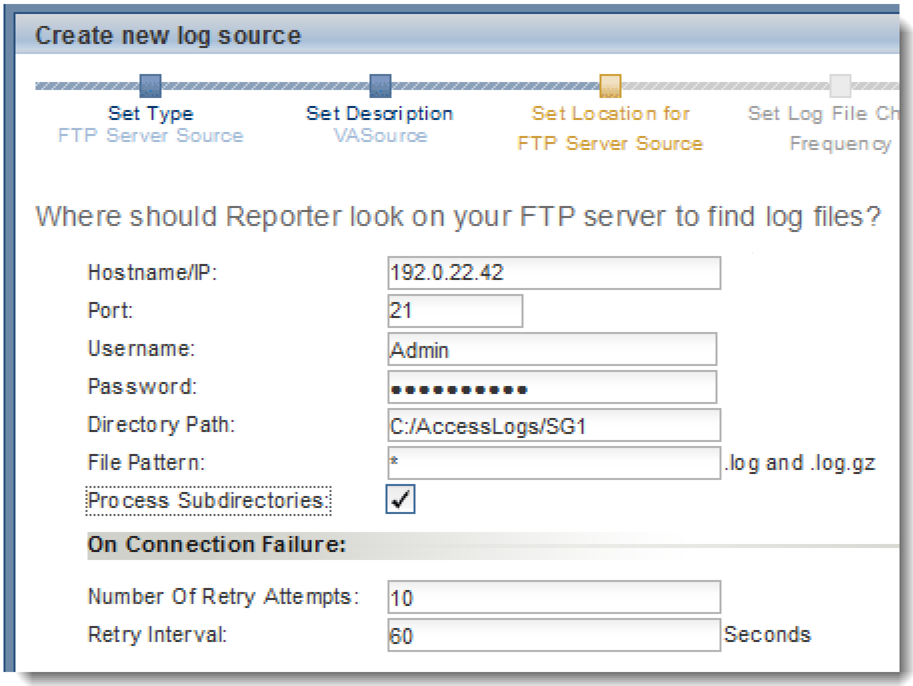
- **FTP Server Source** — If the ProxySG appliance is configured to upload access logs to a dedicated FTP server.
- **Local File Source** — If you configured the ProxySG appliance to upload access logs directly to the Reporter appliance.

b. Click **Next**.

6. **Name** the **Log Source**; click **Next**.
7. If you selected **Local File Source** proceed to Step 9; otherwise, continue to the next step.
8. Enter the **FTP Server Source** attributes.

a. Select **FTP Server Source** and click **Next**.

b. **Name** the log source; click **Next**.



c. Enter the FTP server access credentials (**Hostname/IP**, **Port**, **Username**, and **Password**).

d. Enter the **Directory Path** to the log files on the FTP server.

e. The default **File Pattern** value is an asterisk (*****). For this initial task, Reporter processes all files with the **.log** or **.log.gz** extensions and ignores all other extensions.

f. If the access log directories contain multiple sub-folders, select **Process Subdirectories** to ensure that all content is processed.

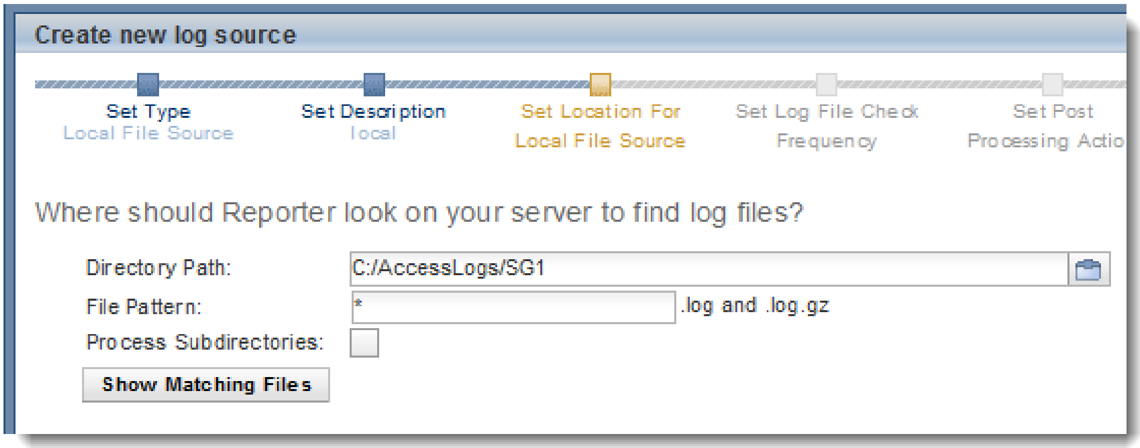
g. (Optional) Edit the **Number of Retry Attempts** and **Retry Interval** settings.

h. (Optional) Click **Show Matching Files** to verify that the specified directory contains the correct files.

i. Click **Next**.

j. Proceed to Step 10.

9. Enter the **Local File Source** location.



a. Enter the **Directory Path** to the log files on this Reporter appliance.

> **Tip:** To create a new directory, click the folder icon.

b. The default **File Pattern** value is an asterisk (*****). For this initial task, Reporter processes all files with the **.log** or **.log.gz** extensions (and ignores all other extensions).

c. If the access log directories contain multiple sub-folders, select **Process Subdirectories** to ensure that all content is processed.

d. (Optional) Click **Show Matching Files** to verify that the specified directory contains the correct files.

e. Click **Next**.

10. (Optional) Specify how often to check this log source for new files. (This setting takes precedence over the schedule in the *Create new database* wizard.)

    - **Use Database Default**— Reporter uses the same setting as specified in the *Create new database* wizard.
    - **Custom Schedule**—Specify check time that is different from the database default. For example, the database checks once daily, but you would like this log source checked only once a week.

    Click **Next**.

11. Specify a post-processing action, or what happens to the log files after Reporter adds the data to the database.

    - **Rename: Append '.done' to the filename** — Reporter appends **`.done`** to the existing **`.gz`** or **`.log`** suffix and leaves the file on the server.
    - **Move to folder**—Reporter moves the log files to the specified directory.

- **Remove: Delete log file**— Reporter deletes the log files from the FTP server directory.

> **Warning:** Select **Remove** only if you are certain that you will never need to process these logs again.

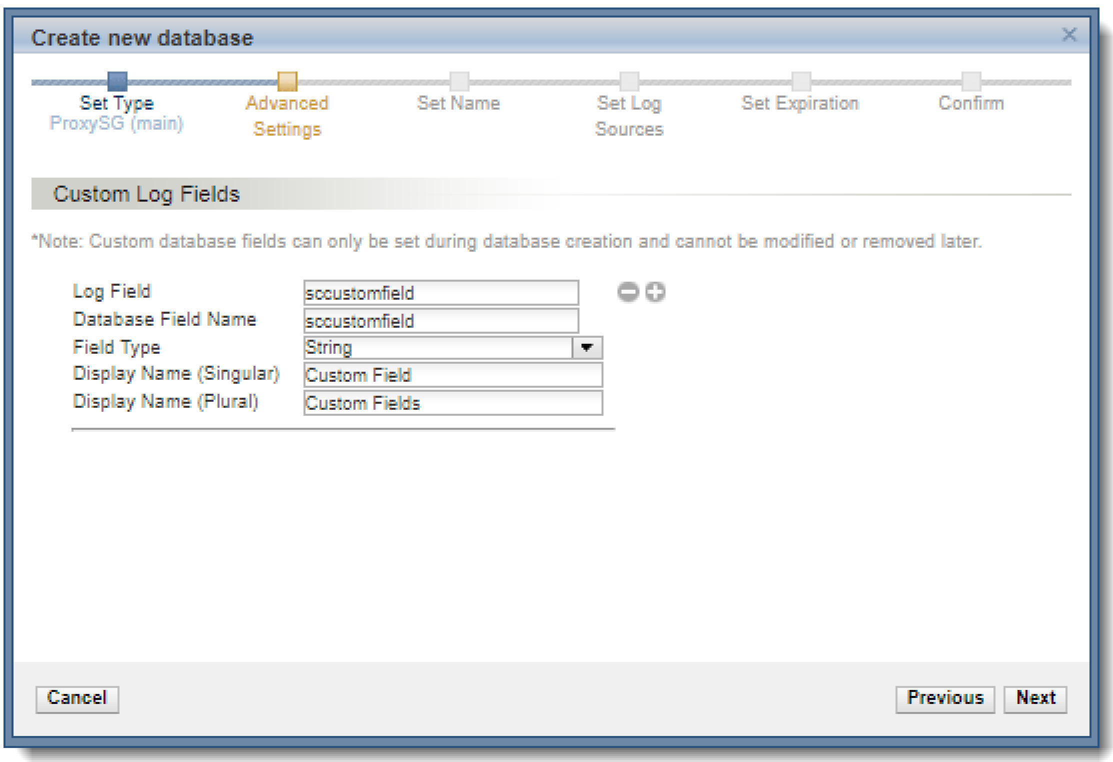
Click **Done** to return to the *Create New Database* wizard. Click **Next**.

12. Specify how long data will remain in the database. Reporter purges data from the database at the specified dates and times.

    During the data purge, Reporter reclaims RAM. Symantec recommends that you schedule large-scale database purging during non-production hours.

    > **Tip:** Reporter expires a database based on the amount of time since the last processed log entry—not on when the database was created.

13. Click **Next** and then click **Done**. Reporter creates the new database with its associated log source.

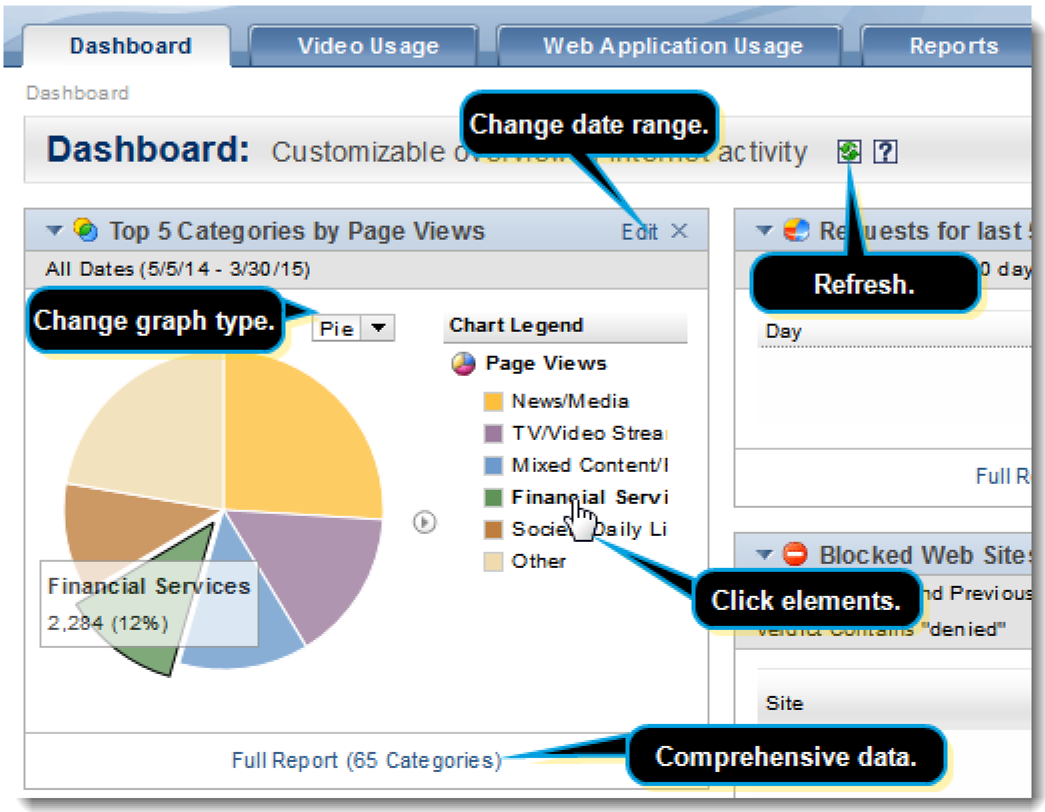


Refer to Other Documentation

With Reporter now deployed, refer to the *Reporter 10.x WebGuide* and the online Help for assistance with further configurations and use.

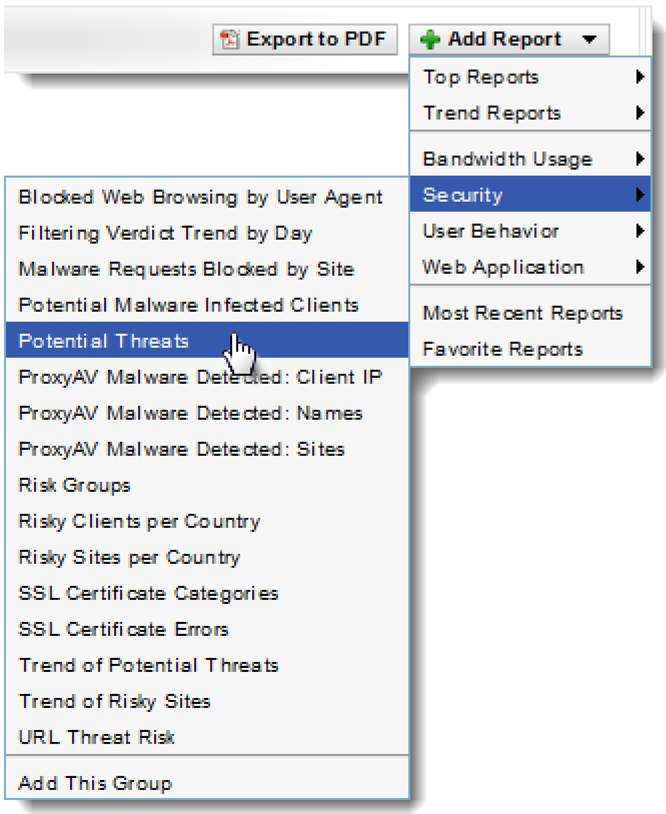
About the Reporter Dashboard

As Reporter builds a database, data begins to populate the dashboard reports.

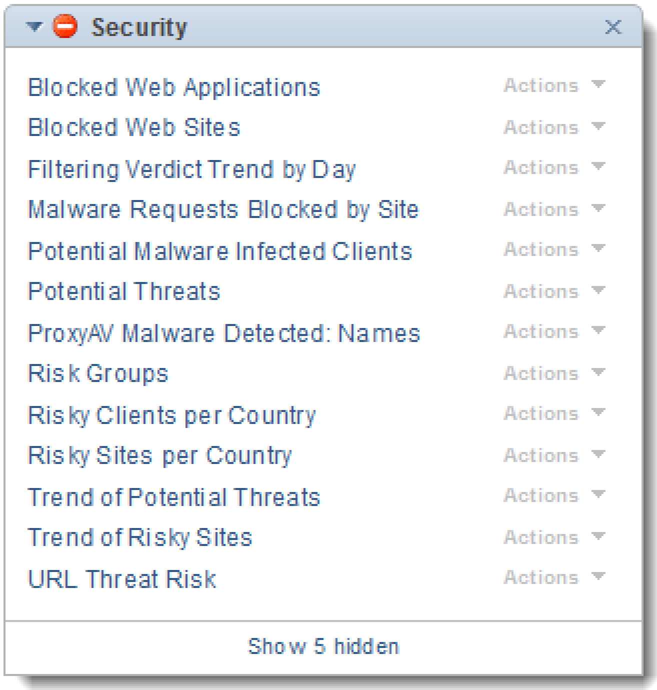


The Reporter dashboard provides a high-level view of web transactions.

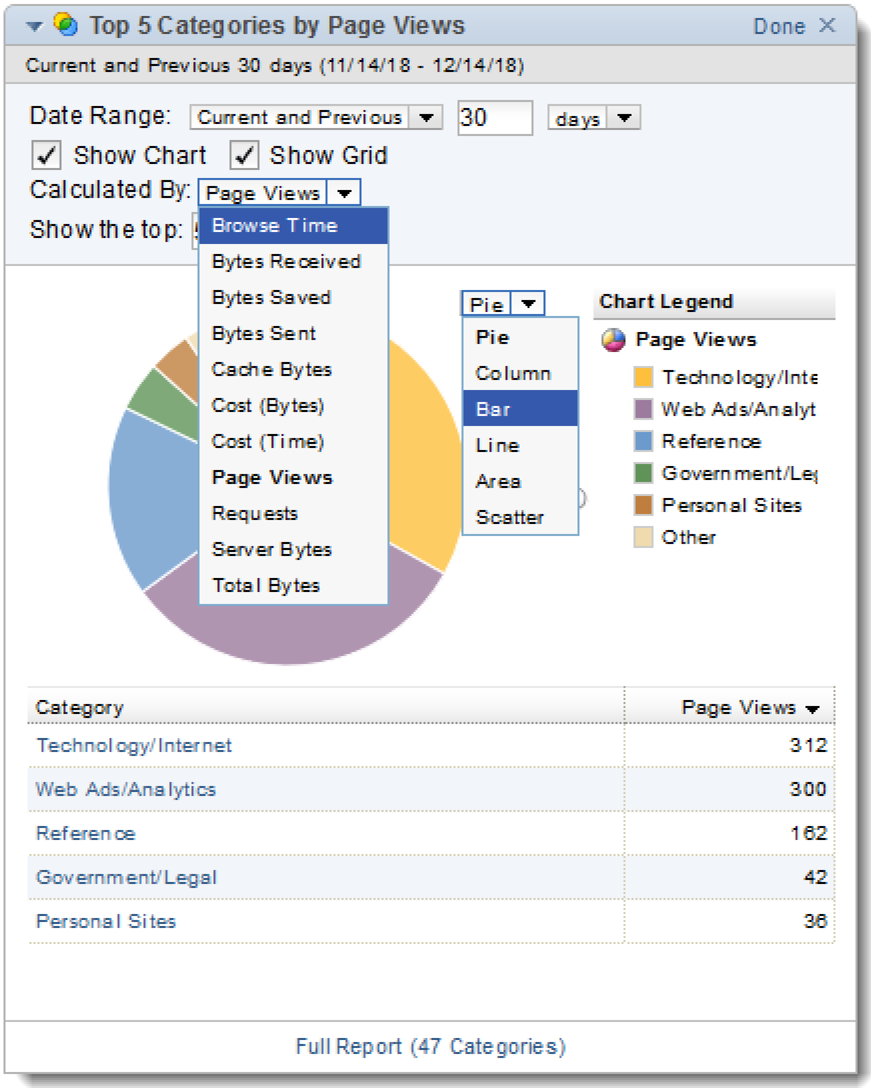
- To add reports to the dashboard click **Add Report** in the upper-right corner.



- Select an individual report to add or select **Add Group** to add a list of reports in a single report widget.



- To customize the report widget click **Edit**.



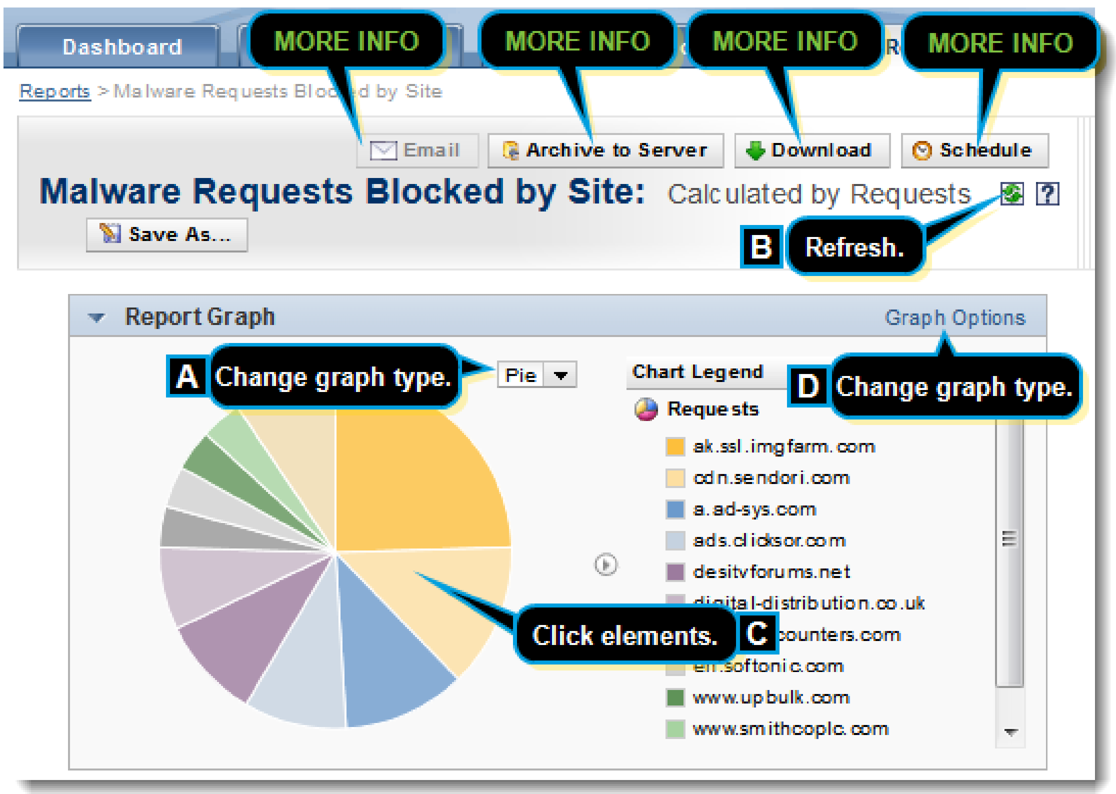
  - Select the **Date Range** to show.
  - Select either **Show Chart** or **Show Grid** or both to display the graphical data representation and the tabular representation, respectively.
  - Select what the data should be **Calculated by** from the drop-down list.
  - For **Show the top** specify how many rows to include in the chart and grid.
  - From the chart's drop-down list select which chart type to display.

What Can I Do From a Report?

Select the **Reports** tab and then click a report name to generate that report. Each generated report provides multiple features and data points.

Manage the Report

Tip: The green MORE INFO elements in the screenshot take you directly to that topic.



A—Each report displays a default graph or chart, based on what Symantec estimated to the best representation. You can change the style from the drop-down list.

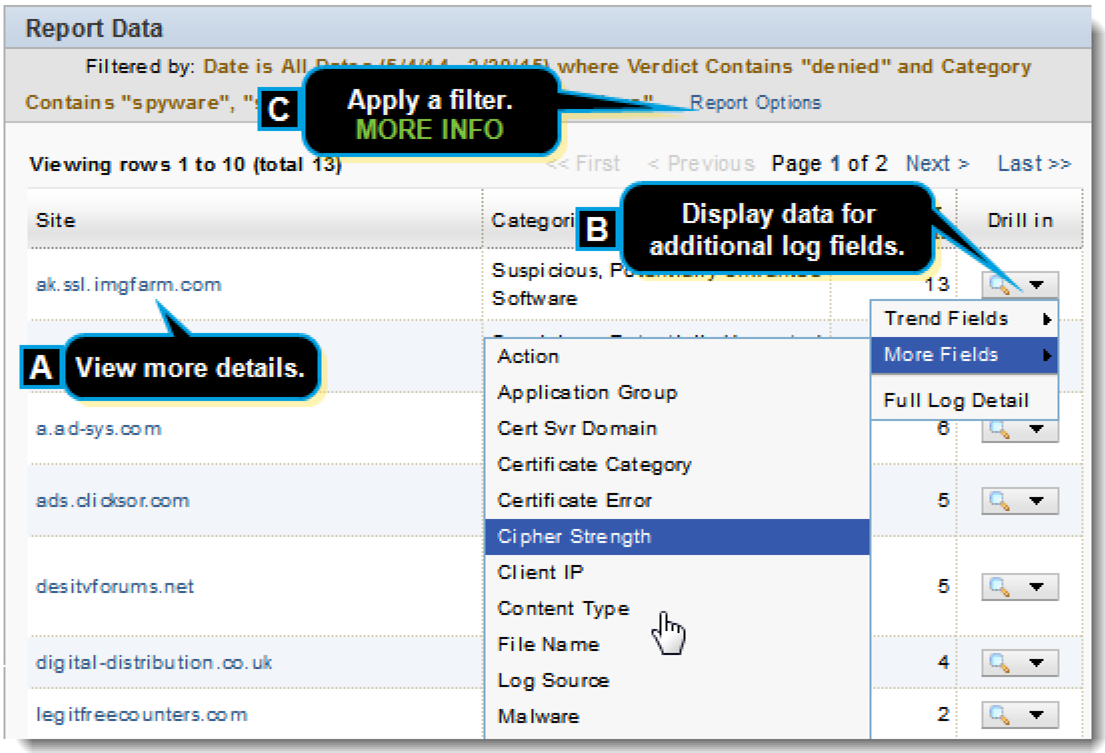
B—To ensure the latest processed data, click the refresh icon.

C—Select elements in the graph or in the data area to highlight it and see more details about that data.

D—Click **Graph Options** to change what data points the graphic contains. Adding or removing data points might change the graphic type.

Drill Down For More Details

Each report contains options to view even more granular data details.



A—Click any blue data link to view more details about that specific element.

B—Use the **Drill In** drop-downs to isolate data. For example, on a particular data element, you want to see what **Users** initiated the request.

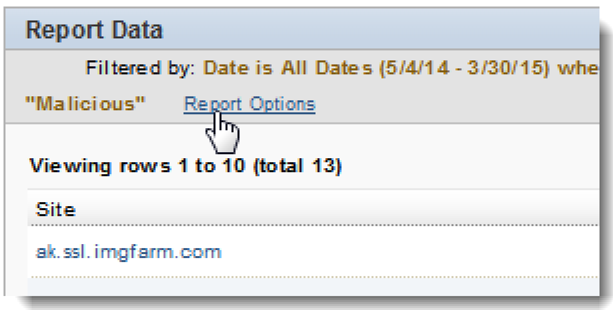
C—See "Apply a Report Filter" on page 18.

Apply a Report Filter

Applying a report filter allows you to narrow the scope of displayed data, based on a specific time frame or another data point, such as a specific user. The filtering mechanism adapts to the data in the report, which enables you to quickly select one or more attributes to include or exclude from a report.

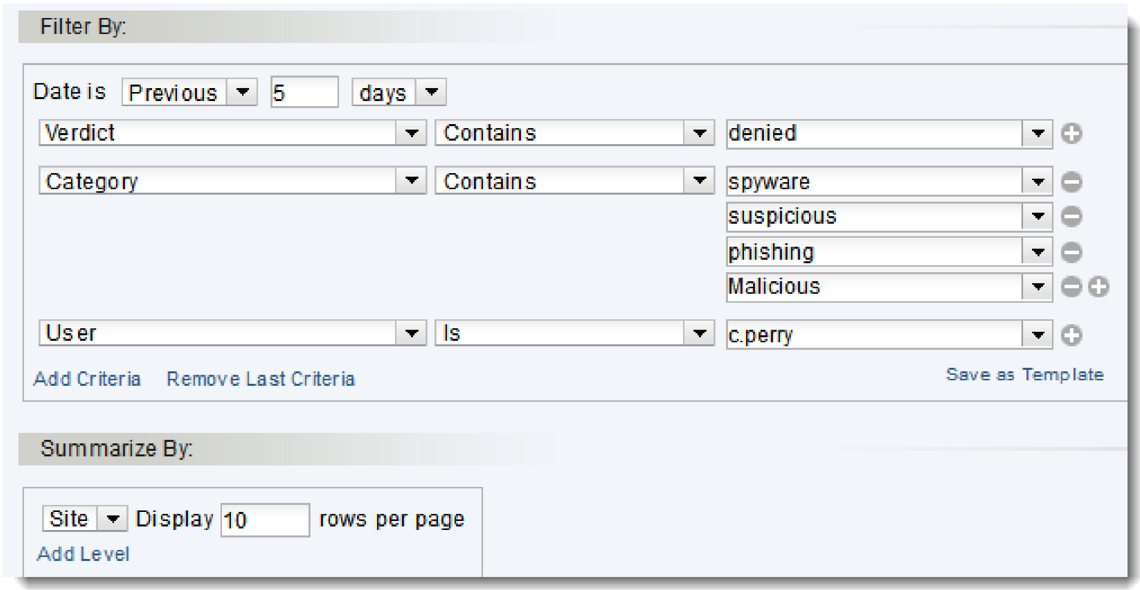
> **Caution:** Some search features and filters, such as the IPv6 filter, will not be available unless Reporter is up-to-date.

To access filter options select the **Reports** tab, click a report, and then click the **Report Options** link in the **Report Data** header.



Filter Options

The filter comprises two sections: date and criteria. You can modify either or both to create a report filter.



1—Date Filter

The default date filter displays data for all dates that are processed in the database. To restrict the report data to specific time frames, select an option from the **Date** drop-down list:

- **Custom**—Allows you to specify a date range.
- **Since**—Displays all data from the specified date to current (or the final date in the access log database).
- **Current**—Displays data only from the current **hour**, **day**, **week**, **month**, or **year** (select one).
- **Previous**—Displays data going back the specified time frame: **hours**, **days**, **weeks**, **months**, or **years** (select one). Partial times are not displayed. For example, if you select the previous week, no current days from the current week display.
- **Current and Previous**—Displays data beginning today and going back the specified time frame: **hours**, **days**, **weeks**, **months**, or **years** (select one). Partial time periods are included. For example, if you select current and previous week, days in the current week display.

As you select each **Date is** option, the field options change. Some fields require you to enter values such as **4** to indicate how many previous days. The other fields display interactive calendars that enable you to quickly select date ranges.

2—Criteria Filter

The default criteria filter displays all data points that are valid for that report; for example, every user name, every category, every user agent, every IPv4 and IPv6 address, and so on. Adding a criteria filter either restricts data to values or excludes data. For example, if you want to see only one user specify **is**, or you want see every user but one specify **is not**, or if you want to see every instance of malware with the keyword **trojan**.

a. From the first drop-down list select the data point.

b. From the second drop-down list select a qualifier (**Is**, **Is not**, **Contains**, **Does not contain**, **Matches regex**, **Does not match regex**).

> **Note:** Using regex (regular expressions) is an advanced technique and is not recommended without extensive knowledge of regex. For more information, see How to create more efficient Regular Expressions.

c. From the third drop-down list, select (or enter) a value. This drop-down list populates with options that are valid for that data point.

> **Tip:** If you know the name of the value and begin entering characters, the field auto-populates with a list of choices present in the database.

d. (Optional) Click the **+** symbol to add additional value fields. The report displays all value matches.

> **Tip:** If you believe you will have future need for this custom filter, click **Save as Template** and name the filter. The next time you need the same filter, click **Load Template** and select it.

f. Click **Apply**.

Use Case: Filter for Users Who Report to Me

This filtering ability requires LDAP implementation (About LDAP Integration). You are a manager and you want to filter the **Web Browsing per User** report to display data only for people who report to you. On the **Web Browsing per User and Category** report, you add a criteria filter with the **User**, **Reports to**, and **Current User** options.

> **Note:** If the username formats in the log files do not match the Reporter username configuration, no data is displayed. See the **Matching the Access Log Username Formats for Filters** section in Manage Existing Databases.

For administrators, Advanced Filtering Tasks provides instructions for creating filters that are more advanced than those you can create in the web interface.

Optimize a Filtered Report

Although Reporter's standard reports are optimized, reports that have additional filters can sometimes take a significant time to run because no data aggregation has been performed. Reporter 10.4 and later allows you to optimize these custom reports, allowing them to run more quickly in the future.

Report Optimization Can Impact Resources

Always consider the database size and current resource state before optimizing a report.

- The report optimization process consumes additional memory and disk resources that can impact current processes. Depending on the size of the database and the number of additional filter criteria, the report operation process can consume significant resource. Always review your **System Diagnostics** (**Administration > System Overview > System Diagnostics**) before optimizing a report.
- Depending on the size of the database, report optimization can sometimes take hours. The database could be suspended during that time. However, only log processing and log expiration are affected and will not resume until optimization is complete.
- Each additional report criteria will increase memory and disk usage.

Some Reports are Not Eligible for Optimization

Consider the following:

- If a report has more than three unique database summary or filter columns, it cannot be optimized.

  For example, a report summarized by user and filtered by user has a single column. It can be optimized. But, a report summarized by site and user, and filtered by category and verdict, has 4 unique columns and cannot be optimized.

- When you optimize a report, time columns are not counted toward the optimization limit.

  For example, consider the following two-level summary report that has:

  - Summary columns for year and week
  - Filters for day of week to exclude Saturday and Sunday
  - Filters on category and verdict

  This report would only require a pair aggregation optimization on category and verdict. This is because time-based columns and filter criteria are not included in the unique column list when searching for an aggregation to use (because the entire database and its aggregations are already organized around per-hour and per-day time periods).

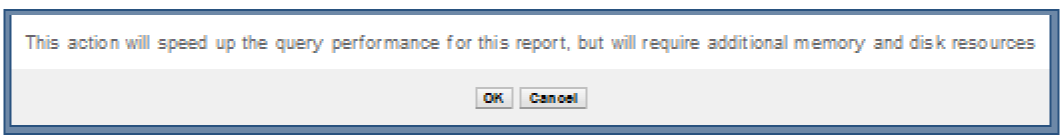
- When you optimize a report, the data for the entire database is optimized, as is all future data for that filter criteria. So, if you optimize a user report filtered by site and later create a site report filtered by user, the site report is already optimized.

Optimize a Report

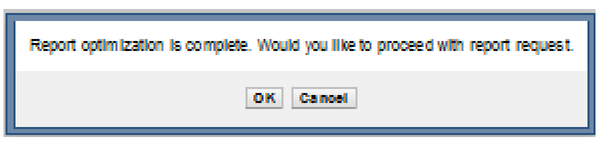
1. Review the "Report Optimization Can Impact Resources" on the previous page.
2. Select the **Reports** tab.
3. Create a new filtered report and save it by clicking **Save As**.

   Alternatively, select an existing custom report.
4. Select **Actions > Optimize**.

5. Confirm that you want to continue with the optimization process.



   The system starts the optimization process.
6. Click **OK** when the optimization is complete to run the report again.



   You'll notice the report completes more quickly.

Undo Report Optimization

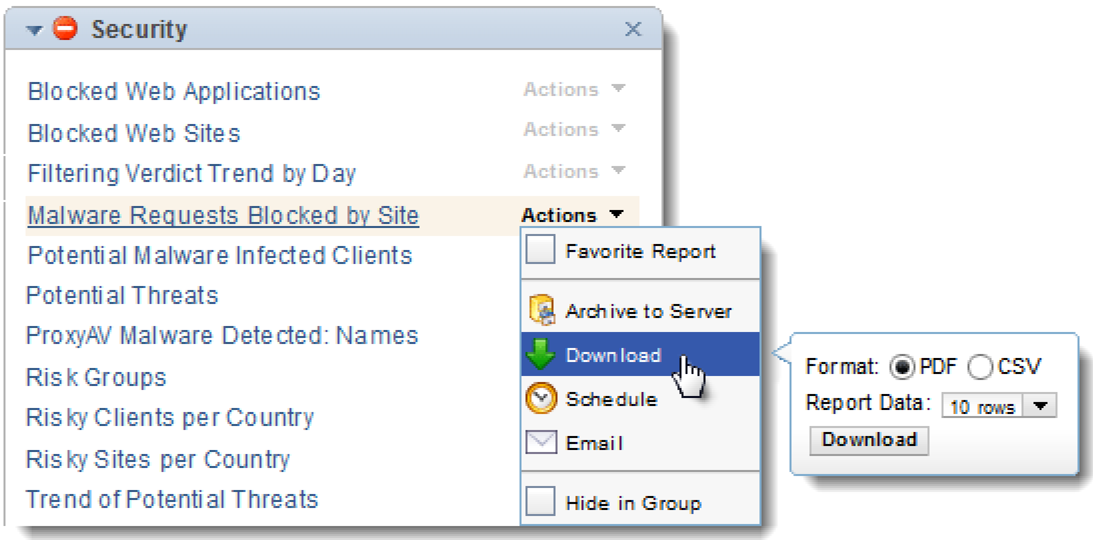
To undo report optimization, you must edit the configuration file as described in Manually Edit Configuration Files and Create Custom Log Fields.

Download a Report

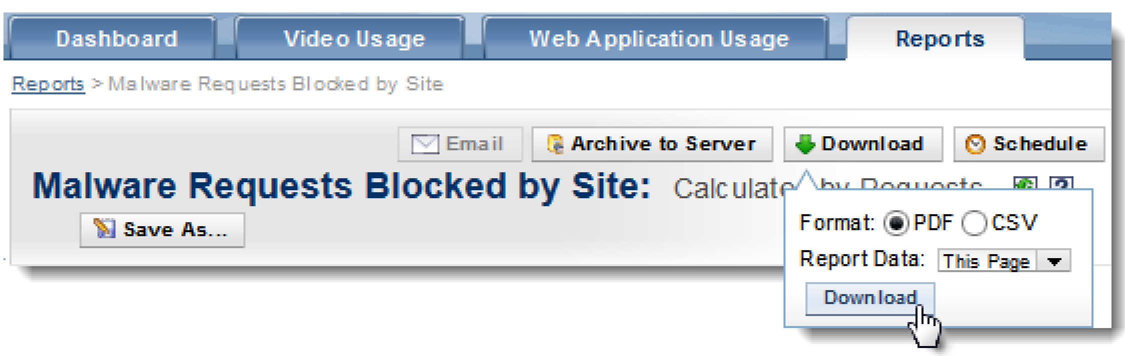
Each top-level report has a **Download** button. Reporter enables you to immediately generate a report as a PDF or a CSV file to download to your local workstation.

1. Access the **Download** control in one of two ways:

   - On the **Reports** tab click **Actions** for a report and then select **Download**.



   - On any generated report, click **Download**.



2. Select the format for the downloaded file:

- **PDF**—Reporter downloads the report as a PDF file.
- **CSV**—Reporter downloads a spreadsheet-compatible file, which contains the report data, with a **.csv** extension. Opening the file requires a spreadsheet application such as Microsoft Excel.

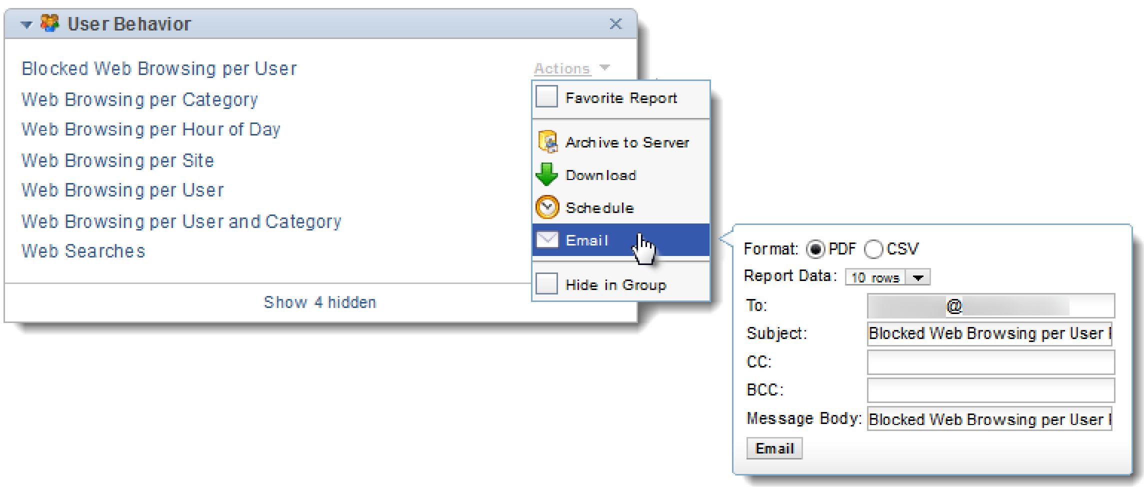
3. From the **Report Data** drop-down list, select how many rows of the report to download.
4. Click **Download**.

Email a Report

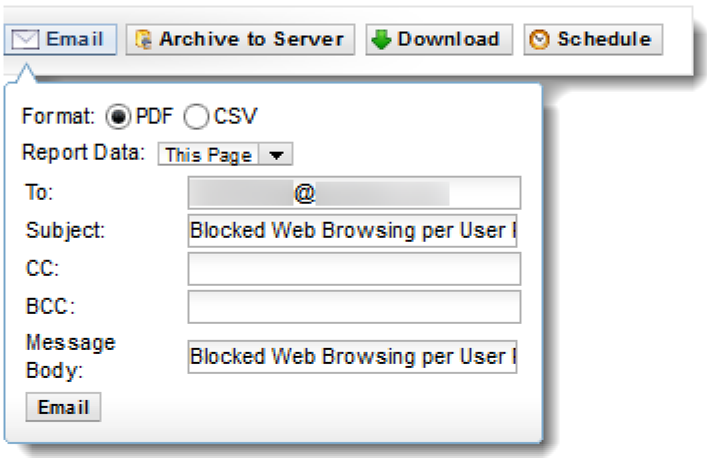
As you are reviewing reports, you might see data that someone else in your organization should see. Reporter enables you to send to a report as a PDF or a CSV file to specified recipients.

> **Note:** If the **Email** button is unavailable, Reporter is not configured with or not able to communicate with the mail server. See Connect Reporter to an Email Server.

1. Access the **Download** control in one of two ways:
   - On the **Reports** tab click **Actions** for a report and then select **Email**.



- On any generated report, click **Email**.



2. Select the format for the file:

   - **PDF**—Reporter attaches a PDF file to the email. The recipient must have Adobe Acrobat to view the file.
   - **CSV**— Reporter attaches a file of the report data with a **.csv** extension. The recipient can open the file with a spreadsheet application such as Microsoft Excel.

3. From the **Report Data** drop-down list, select how many rows to include in the report.
4. In the **To** field, enter the valid email address of the intended recipients. Separate multiple recipients with commas (**,**).

   > **Note:** The **From** address will be the address that the administrator configured on *Administration > General Settings > Reporter Settings > System Settings > External Servers > Email*.

5. The default value in the **Subject** field is the full name of the report. Accept this value or enter a new subject line.
6. (Optional) Enter email addresses in the **CC** (carbon copy) and **BCC** (blind carbon copy) recipient fields.
7. The default value in the **Message Body** field is the name of the report plus the word **attached**. Accept this value, modify the text, or enter a new message body.
8. Click **Email**. Reporter emails the report to the recipients.

Archive a Report

As you are reviewing reports, you might determine that a specific report needs to be permanently stored for future reference. Your Reporter administrator might have configured Reporter to not process access log data that is older than a specific time; archiving a report is a way to preserve that data. Consider, however, that the Reporter administrator has the ability to delete archived reports to maintain disk-space capacity. Communicate with your administrator if there is a report that absolutely must remain archived. Reporter enables you to archive to a report as a PDF or a spreadsheet-compatible database file.

About Export to PDF

Some special characters that are displayed in reports might not be displayed in exported PDF files. Be advised of the following when Reporter is set to specific languages.

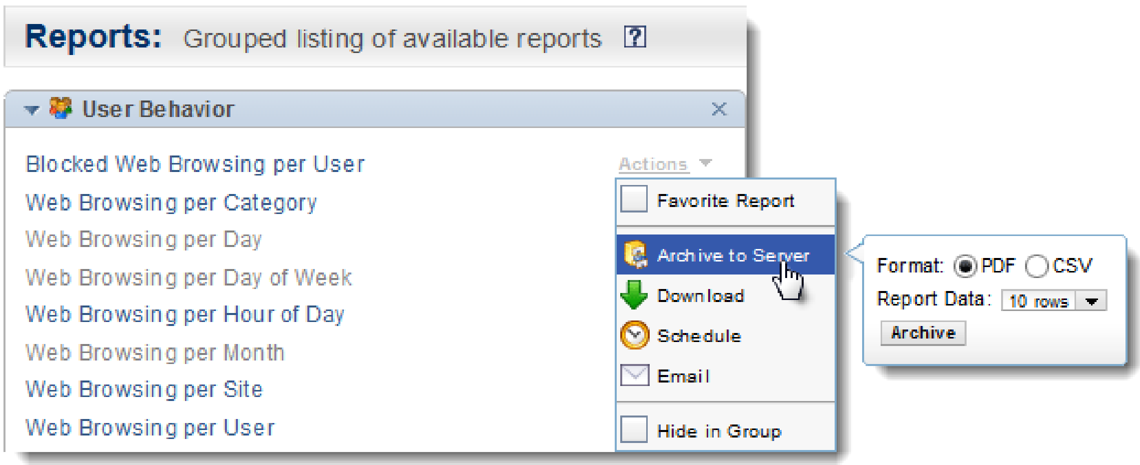
- **English**—Reporter displays all data values using Mac OS Roman encoding (upper-ASCII Latin characters). The character reference: http://en.wikipidia.org/wiki/Mac_OS_Roman. On this page (as of this production date), the lower-ASCII (rows 2–7, excluding control characters) and the orange background characters. Reporter does support the upper-ASCII math symbols or the Apple character.
- **Japanese**—Reporter displays the values using the HeiseiMin-W3 font.
- **Chinese (simple)**—Reporter displays values using the STSong-Light font.
- **Chinese (traditional)**—Reporter displays values using the MSung-Light font.

Adobe provides all of these fonts for PDF display.

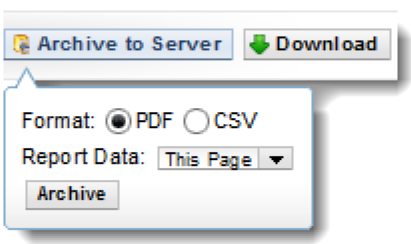
Procedure

1. Access the **Archive** control in one of two ways:

   - On the **Reports** tab click **Actions** for a report and then select **Archive to Server**.



   - On any generated report in the **Reports** tab click **Archive to Server**.



2. Select the format to archive the file:

   - **PDF**—Reporter archives the report as a PDF file.
   - **CSV**—Reporter archives a file that contains the report data with a **.csv** extension. Opening the file requires a spreadsheet application such as Microsoft Excel.

3. From the **Report Data** drop-down list, select how many rows of the report to include in the archive.

4. Click **Archive**. The report is archived on the Reporter system on the main **Reports** tab in the **Archived Reports** group. From there, you can access or delete the report from the archive.

In Brief: Content Analysis + MA Database

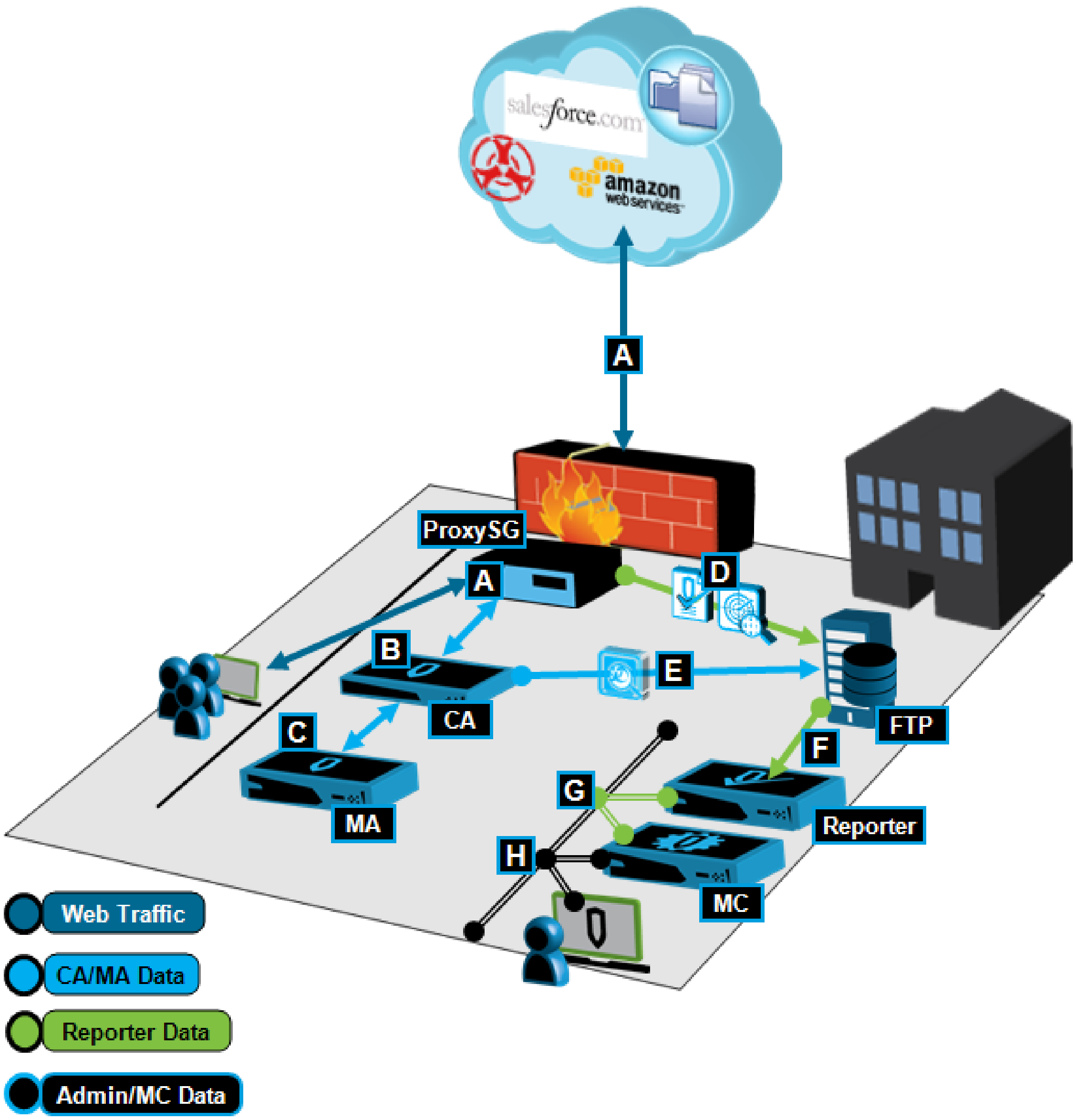
You can create a database that includes malware scanning and sandboxing results from the Symantec Content Analysis and Malware Analysis appliances that are deployed as part of your Symantec security solution. This allows you to use Symantec Management Center to view *Unified Threat Reporting*.

> **Note:** FireEye and LastLine integrations also supported. See "Malware Notes" on page 33, below.

This Topic Brief provides a solution overview, component requirements, and the Reporter configuration.

Solution Overview

When all of the Symantec devices are deployed and communicating, the solution consists of aggregated data and Content Analysis sandboxing detonation results that are passed from the gateway SGOS device (for example, ProxySG appliance or Advanced Secure Gateway) through Reporter to Management Center.



A—Clients initiate web requests. The ProxySG appliance compares the content against the Symantec WebFiltering WebPulse databases. If the result recognizes the domain hosting the file as a known malware source, the ProxySG appliance denies the download and notifies the user. If the domain is not recognized, the ProxySG appliance sends the file to Content Analysis for inspection.

B—Actions:

- If Content Analysis detects malicious content, it performs the configured action (Allow or Block) and notifies the SGOS device of the activity.

- When Content Analysis detects a suspicious file (executable or a common malware attack vector) that does not match any known malware signatures or triggers a malware score from static analysis or that is *not* on the whitelist, the appliance forwards the file to the Malware Analysis appliance, if configured

C—Malware Analysis identifies the actions an executable file would take on a client workstation, including malicious URL web requests and changes to system files. It evaluates the threat of a given file and provides a threat score as a number between 1 and 10. The higher the number, the greater the threat. The Content Analysis sends the detection results (ultimately destined for Reporter) to the ProxySG appliance.

D—The ProxySG appliance uploads transaction logs (**bcreportermain_v1**) to the staging FTP server.

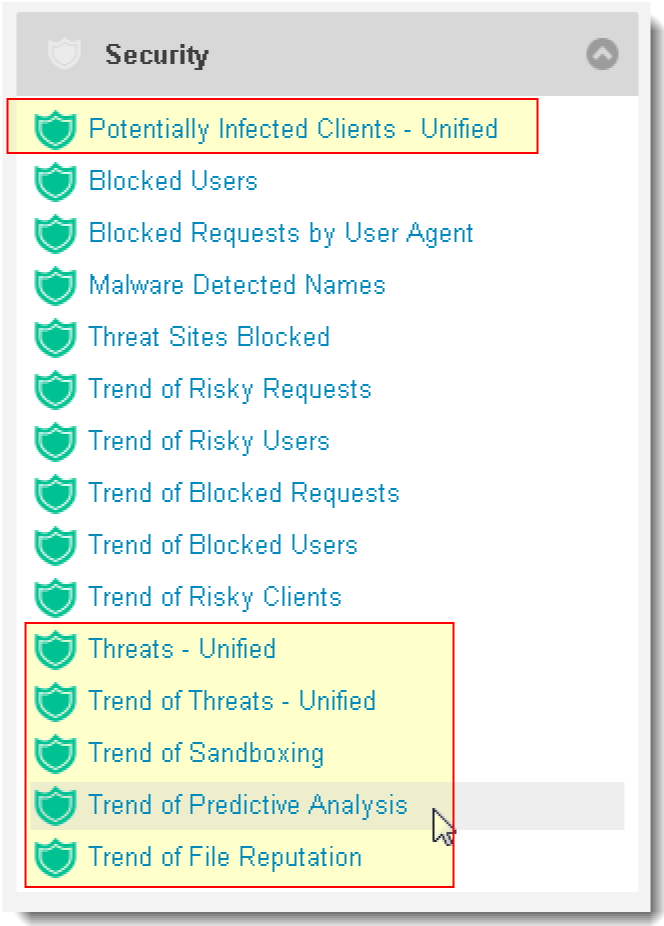
- This data set is the result of the data the ProxySG appliance collects directly, as well as the results of Content Analysis antivirus scanning. New access log fields: **`x-file-reputation-score`**, **`x-cylance-score`**, **`x-cas-date`**, **`x-cas-time`**, **`x-event-id`**. If real-time sandboxing is enabled, the results include a general score and whether or not additional sandbox results are coming (see **E** below).
- The upload also contains the standard transaction details used for standard reporting.

E—When additional sandboxing results occur, the Content Analysis uploads those results to the Reporter FTP server (see "Other Documentation Resources" on page 35 for a link to this procedure).

F—When the Reporter database pulls the data from the FTP server, a new field (**`x-bluecoat-transaction-uuid`**), Reporter reconciles and consolidates the ProxySG-source and Content Analysis-source data.

G—When added as a device, Reporter provides the processed access log data to SymantecManagement Center.

H—The Admin views Content Analysis —and possibly Malware Analysis detonation—results in supported reports.



- **Potentially Infected Clients - Unified**
- **Threats - Unified**
- **Trend of Threats - Unified**
- **Trend of Sandboxing**
- **Trend of Predictive Analysis**
- **Trend of File Reputation**

Malware Notes

- Risk scores 7 or higher are considered malicious (this threshold is configurable on Content Analysis).
- Malware Analysis indicators—If Malware Analysis processing results in a detonation, the Malware Analysis sends that result to Content Analysis, which notifies the SGOS proxy device. The SGOS proxy device caches the result

and blocks subsequent requests that match. However, the log entries for these cache block actions do not contain the sandboxing vendor or score. Because of this, you might not see the Malware Analysis benefits reflected in the reports. For example, the SGOS proxy device might block 20 requests that match a cached result; the Malware Analysis is credited with only one result (the one that resulted in the cache entry). When the SGOS proxy device receives a clear cache action (for example, when new AV patterns are loaded), the Malware Analysis action re-occurs on the next request.

- If the solution involves integration with FireEye® or Lastline® sandbox vendors, those results are included. Each vendor employs different Risk Score scales.
    - **FireEye**—A **0** score is safe; a **1** score is malicious.
    - **Lastline**—Employs a scale of **0** (safe) to **100** (malicious).

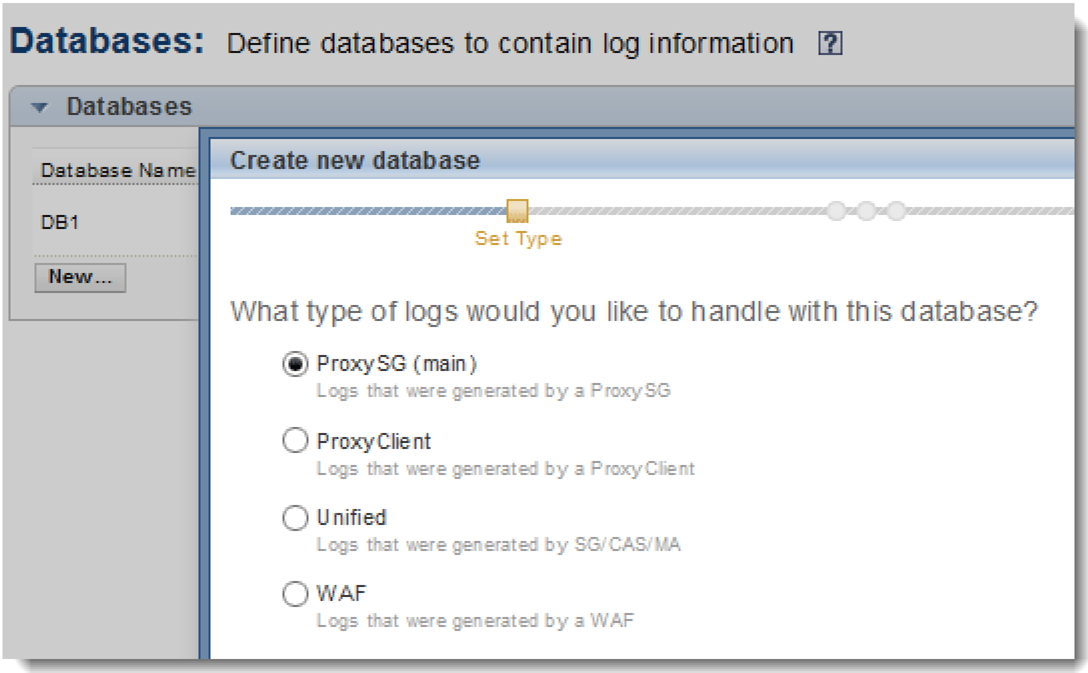
  To make the results consistent for Symantec's Risk Scoring, the FireEye score is multiplied by ten. The Lastline score is divided by ten.

Requirements

- ProxySG appliance minimum versions—SGOS 6.6.4.x or 6.5.9.2.
- Content Analysis—1.3.6.1
- Malware Analysis—Any current version
- Reporter minimum version—10.1.4.x, which provides the **`x-bluecoat-transaction-uuid`** field.
- Management Center minimum version—1.5, which provides the enhanced reports.

Reporter Configuration

The only required Reporter configuration is to create a new database and select the **Unified** database format.



a. In Admin mode, select **General Settings > Reporter Settings > Data Settings > Databases**.

b. Click **New**. Reporter displays the *Create New Database* dialog.

c. Select **Unified**.

d. Continue database configuration.

Reporter Notes

- You cannot view Unified reports from the Reporter interface; you must use Management Center.
- If you create Unified DB databases, the **View Reports** link is not available.

Other Documentation Resources

- [Content Analysis]

  Procedure for sending sandbox results to the Reporter FTP server: [CAS to Reporter Topic].

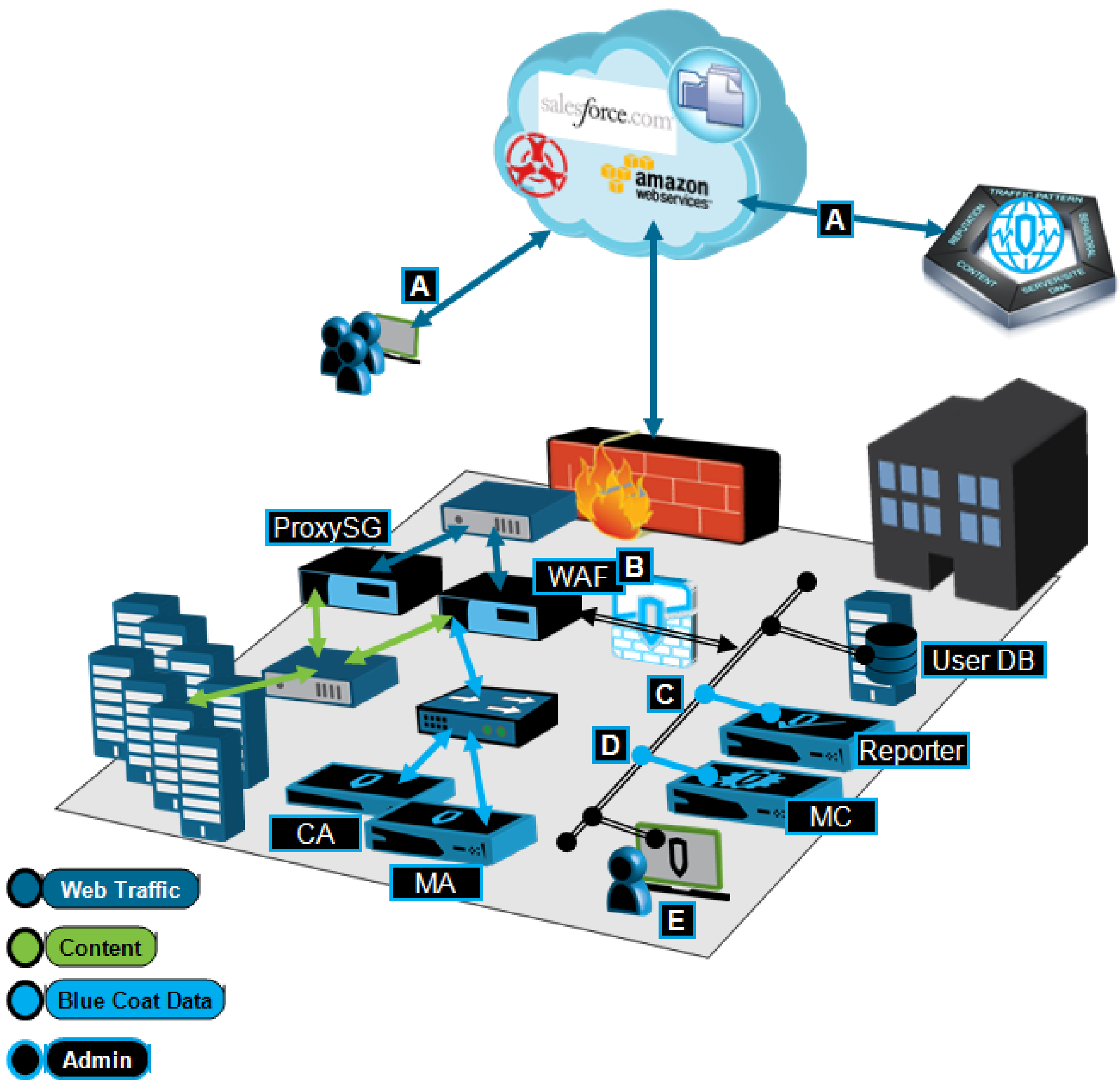
Symantec Reporter 10.4.1.1

- Malware Analysis
- Management Center

In Brief: WAF Reporting Database

Create a database that enables Web Application Firewall (WAF) reporting to use Symantec Management Center to view WAF reports, analyze, and adjust policy accordingly across the ProxySG devices performing in WAF roles.

Topography



A—Clients initiate web requests; the Symantec Global Intelligence Network™ (GIN) provides website and web application ratings and categorizations.

B—Integrated with Symantec Content Analysis and Malware Analysis appliances, the ProxySG appliances in WAF roles protect content servers. The ProxySG appliances upload the WAF access log format (**bcreporterwarp_v1**) access logs to an FTP staging server.

C—Symantec Reporter compiles a WAF database (requires a database created specifically for WAF).

D—Symantec Management Center, with Reporter added as a device, generates **Security** reports that contain WAF data.

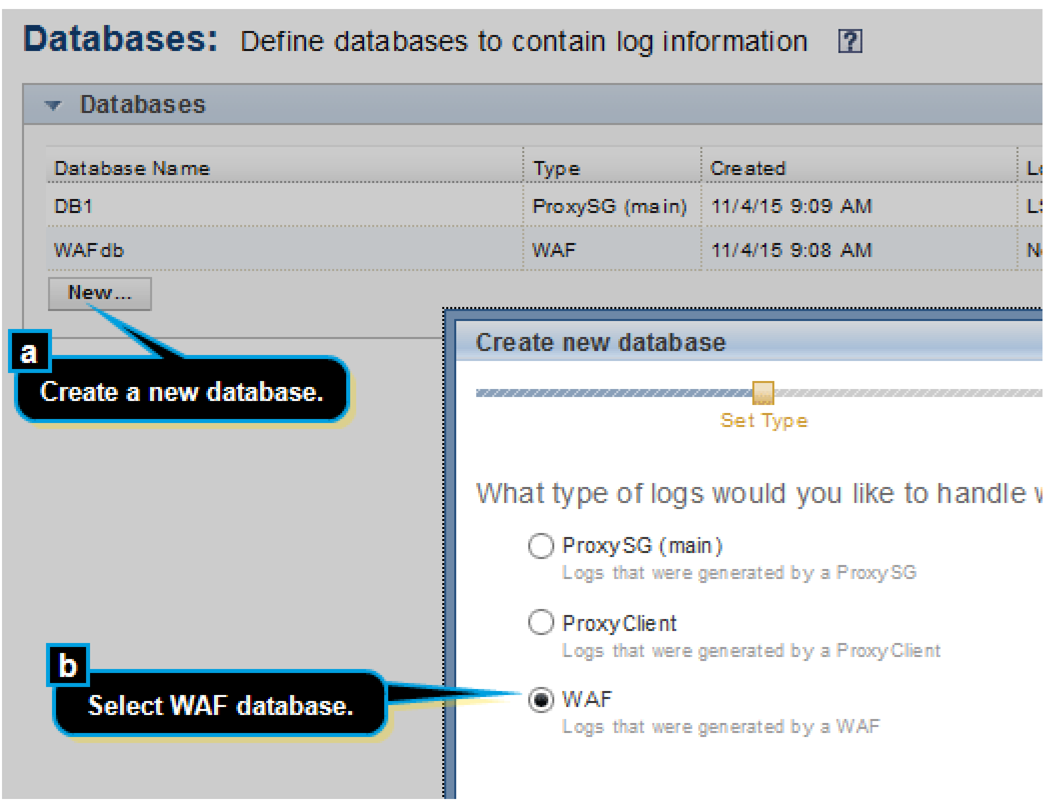
E—The IT Admin accesses Management Center to view the reports, analyze, and adjust policies accordingly.

Requirements

- ProxySG appliance: SGOS 6.6.3.
- Reporter: The minimum version is 10.1.3, which provides the new WAF database.
- Management Center: The minimum version is 1.5, which provides the new WAF reports.

Reporter Configuration

1. Create the WAF database.



   a. As the administratior select **General Settings > Reporter Settings > Data Settings > Databases**.

   b. Click **New**. Reporter displays the *Create New Database* dialog.

   c. Select **WAF**.

   d. Continue with the database configuration.

2. You must create a role for the user who has access to this Reporter WAF database. This is required for the Management Center operations.

   a. Select **Admin > Reporter Settings > General Settings > Access Controls > Roles**.

   b. Click **New**. Reporter displays the *Create New Role* dialog.

   c. **Name** the role and click **Next**.

   d. On the *Set Permissions* screen, select the WAF database that you created.

      Reporter displays a set of selectable options.

   e. Under **Filter**, select **User**, **Is**, and the username.

   f. Click **Done**.

3. In Management Center, when you add the Reporter appliance, provide this username and password to access Reporter.

Notes

- You cannot view WAF reports from the Reporter interface; you must use Management Center.
- If you create WAF databases, the **View Reports** link is not available.

Other Documentation Resources

- Management CenterReport Descriptions—The **Security** section contains the WAF report descriptions.
- Management Center documentation: Symantec Documentation.

Reference: Ports and Protocols

Consult these tables when deploying Reporter behind a firewall or proxy.

> **Note:** These are the default ports. Some ports can be changed and others not used, depending on your deployment.

Inbound Connections

Service	Port(s)	Protocol	Configurable	Destination	Description
Web UI/API	8081	TCP	Yes	Admin	HTTP UI access - redirects to HTTPS
Web UI/API SSL	8082	TCP	No	Admin	HTTPS UI access (encrypted)
FTP	21	TCP	Yes	Local / accesslogs directory	Non-secure access logs file uploads/downloads/inspection
FTPS	990	TCP	Yes	Local / accesslogs directory	Secure access logs file uploads/downloads/inspection
CLI SSH	22	TCP	No	Admin	CLI management shell access

Outbound Connections

Service	Port(s)	Protocol	Configurable	Destination	Description
LDAP	389	TCP	Yes	LDAP server	User authentication
LDAPS	636	TCP	Yes	LDAP server (encrypted)	User authentication
SMTP	25	TCP	No	SMTP server	Emails, reports, and event notifications
HTTPS	443	TCP	No	Symantec	Licensing and updates for products, subscriptions, ect..

Symantec Reporter 10.4.1.1

Service	Port(s)	Protocol	Configurable	Destination	Description
DNS	53	UDP/TCP	No	Domain name server	Hostname resolution
FTP	21	TCP	Yes	FTP log file server	Access log file upload
NTP	123	UDP	No	Time server	Network time synching
SNMP trap	162	TCP	Yes	SNMP trap server	SNMP communication
syslog	514	UDP/TCP	Yes	syslog server(s)	Sending syslog messages to remote host (disabled by default)
Cloud log download	443	TCP	No	Symantec WSS	Request download of archived access logs from the Cloud Reporting service

Required IP Addresses and URLs

URL	Protocol	Description
`support.symantec.com`	`https/TCP 443`	Support links to software, support cases, and documentation.
`upload.bluecoat.com`	`https/TCP 443`	Upload portal logs and other large files.
`download.bluecoat.com`	`http/TCP 80`	Licensing portal; redirects to **`support.symantec.com`**
`esdhttp.flexnetoperations.com`	`https/TCP 443`	Software portal.
`device-services.es.bluecoat.com`	`https/TCP 443`	License related.