Web Security Service

Hosted Reporting Guide

Version 6.10.4.1/OCT.12.2018

Symantec.™

Copyrights

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com

Web Security Service Hosted Reporting

The Symantec Web Security Service solutions provide real-time protection against web-borne threats. As a cloud-based product, the Web Security Service leverages Symantec's proven security technology as well as the WebPulse™ cloud community of over 75 million users.

With extensive web application controls and detailed reporting features, IT administrators can use the Web Security Service to create and enforce granular policies that are instantly applied to all covered users, including fixed locations and roaming users.

This document describes how to send logs from an existing Symantec ProxySG appliance to the Web Security Service for security scanning and policy checks.

- "About Cloud Service Hosted Reporting" on page 7
- "Configure..." on page 9
- "About Reporting" on page 27

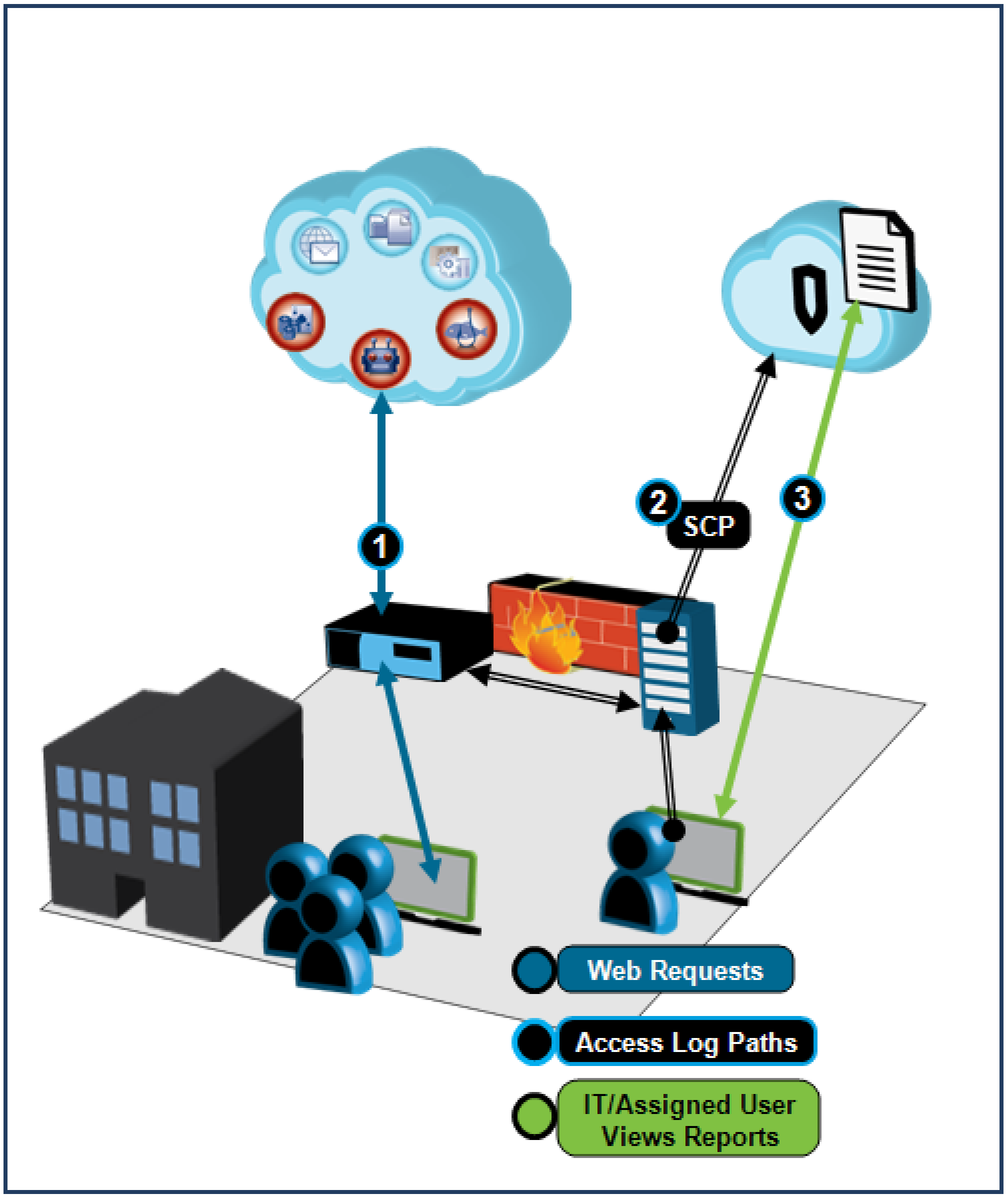
This document contains topics collected from the Web Security Service online documentation. For the complete doc set, see:

Symantec Support Site > WSS Documentation

Table Of Contents

About Cloud Service Hosted Reporting

Hosted reporting provides an alternate to deploying and maintaining Symantec Reporter or other reporting application. Rather than directly processing employee web requests and applying policy checks for security and malware, the Symantec Web Security Service processes the access logs from an existing ProxySG appliance gateway deployment.



Instead of forwarding client Web requests directly to the Web Security Service for processing:

- **1**—The ProxySG performs its standard operation: it processes web requests (authorizes, checks policy).
- **2**—The ProxySG records each web transaction in the **main**-format access logs. The upload client sends the access logs to a Web staging server (HTTP or FTP). A network manager configures a secure copy (SCP) link from the staging server to the Web Security Service service. The service checks every hour for new data.
- **3**—Web Security Service administrators or other personnel in the Reporting User role log into the service to generate and view reports (or have reports sent to them at scheduled times).

The Web Security Service retains live reportable data for one year (in comparison, the Proxy Forwarding access method retains web use data for 90 days).

First Step

Plan the hosted reporting deployment. See "Plan The Hosted Reporting Configuration" on page 10.

Configure...

The section describes how to enable Hosted Reporting on the Web Security Service.

Plan The Hosted Reporting Configuration

The Symantec Web Security Service supports hosted reporting, which means forwarding web use access logs from a ProxySG appliance to the cloud-based service and viewing reports in the Web Security Service interface.

Before beginning device configuration, Symantec recommends that you pre-record the required information. The planning sheet provides default information and forms for you to enter information specific to your network.

Component	Comments	Value
Welcome letter	Provides the initial admin access information.	E-mail: ____ Subscription ID:________________________________
Staging Server Type		__ **Linux** __ **Windows**
Staging Server Protocol		__ **HTTP** __ **FTP**
Staging Server IP Address	Server must have Internet access.	IP address:
Staging Sever Credentials	Required if the server is password protected.	Username: Password:
Staging Folder Path(s)	You might create different folders for different gateway ProxySG appliances, which helps identify logs by site, building, and so on.	Example: **c\Dailylogs4WSS\SanJose**

Next Step

Proceed to "Initial Hosted Reporting Configuration" on the facing page.

Initial Hosted Reporting Configuration

Accessing the Symantec Web Security Service for the first time displays the first page of the Initial Configuration Wizard.

Prerequisite for New Web Security Service Accounts

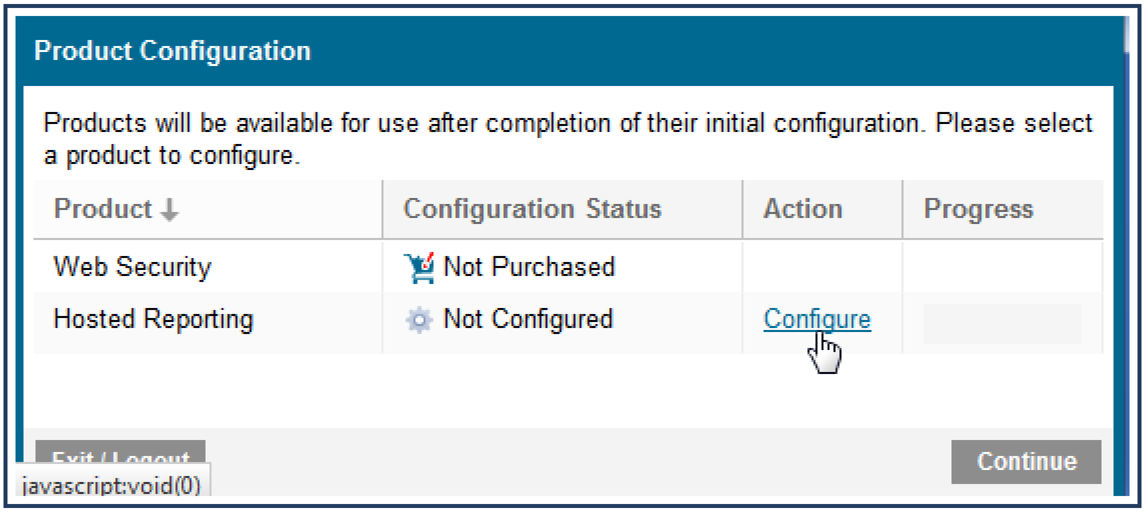
1. In a browser, enter https://portal.threatpulse.com/register .
2. Perform the following:
   a. Symantec strongly recommends reviewing the **Blue Coat Cloud Service Agreement**.
   b. Enter the e-mail address to be associated with the Web Security Service service; for example, the address of the Web Security Service administrator for your company.
   c. Enter your subscription identification.
   d. Click **Next**.

The first page begins the registration/initial configuration wizard. Proceed to the next section.

Follow the Initial Configuration Wizard

The following steps describe the purpose of each page in the wizard. Click **Next** after completing each wizard page. If you are not currently logged in to the service, do so now.

1. To begin the initial configuration wizard, click the **Configure** link in the **Hosted Reporting** product row.



Product Configuration

Products will be available for use after completion of their initial configuration. Please select a product to configure.

Product ↓	Configuration Status	Action	Progress
Web Security	Not Purchased		
Hosted Reporting	Not Configured	Configure	

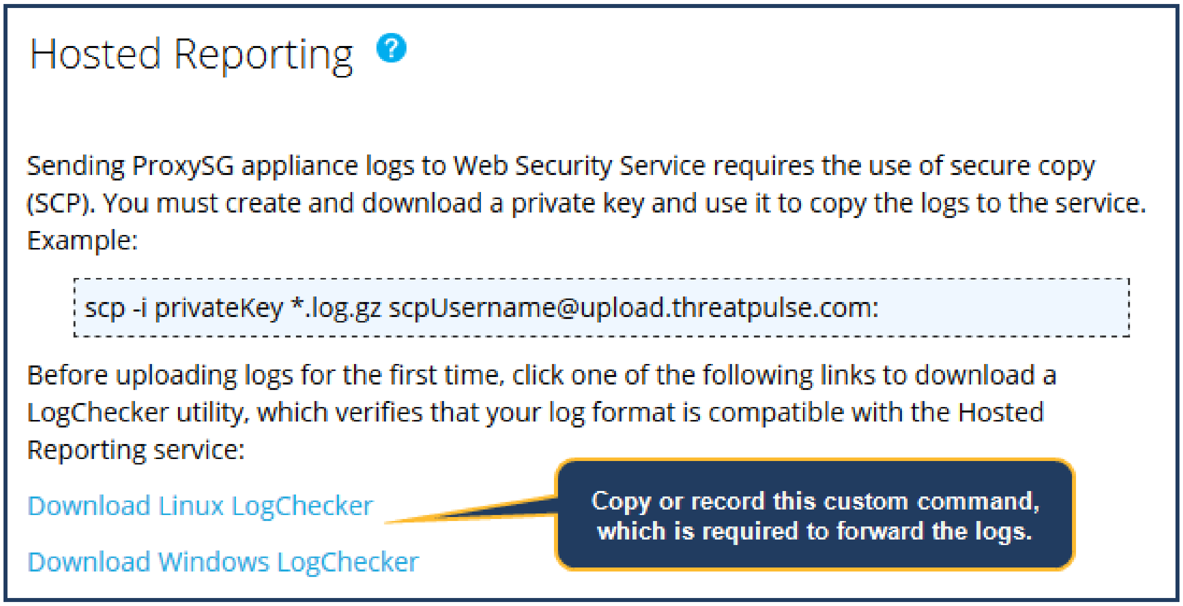
> **Tip:** If you close the browser during the initial configuration process, then return to `https://portal.threatpulse.com`, the **Status** column displays **Config in Progress**. Click the **Configure** link to resume the process from the previously configured wizard page.

2. Each Web Security Service customer account receives a private key command that is used to secure copy (scp) your location's access logs to the service. The format of this command is:

```
scp -i privateKey *.log.gz scpUsername@upload.threatpulse.com:
```

where *scpUsername* is a unique customer identification value provisioned to you by Symantec.

The command displays on the Hosted Reporting initial configuration page. Copy or record this `scp` command, as you will need it when you are ready to forward logs to the service.



Hosted Reporting

Sending ProxySG appliance logs to Web Security Service requires the use of secure copy (SCP). You must create and download a private key and use it to copy the logs to the service. Example:

```
scp -i privateKey *.log.gz scpUsername@upload.threatpulse.com:
```

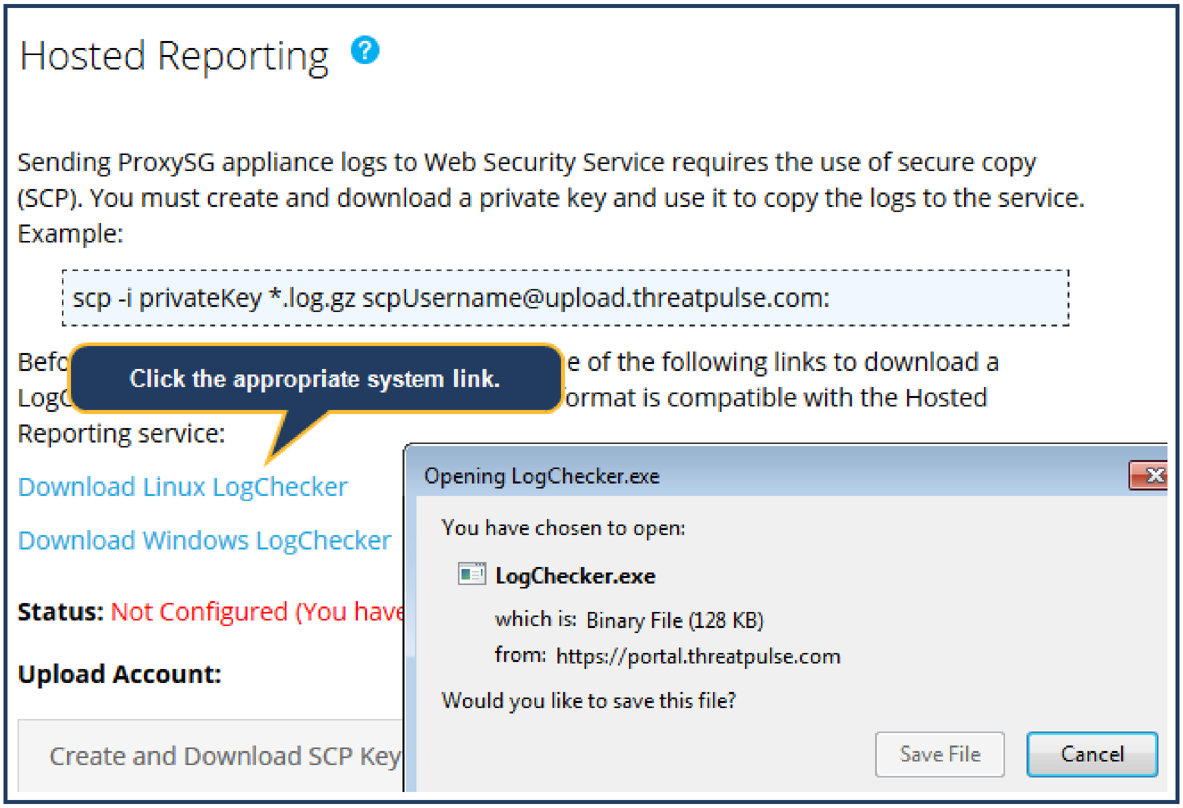
Before uploading logs for the first time, click one of the following links to download a LogChecker utility, which verifies that your log format is compatible with the Hosted Reporting service:

Download Linux LogChecker

Download Windows LogChecker

Copy or record this custom command, which is required to forward the logs.

3. The Web Security Service supports ProxySG main format (ELFF) log files. Before uploading access logs to the Web Security Service service from the staging sever, Symantec recommends running the **LogChecker** application to verify that they are the correct format. You cannot do this until you have staged logs, but for now download the **LogChecker** application to the staging server that contains the logs.



Hosted Reporting

Sending ProxySG appliance logs to Web Security Service requires the use of secure copy (SCP). You must create and download a private key and use it to copy the logs to the service. Example:

```
scp -i privateKey *.log.gz scpUsername@upload.threatpulse.com:
```

Befo... e of the following links to download a LogC... ormat is compatible with the Hosted Reporting service:

Click the appropriate system link.

Download Linux LogChecker

Download Windows LogChecker

Status: Not Configured (You have

Upload Account:

Opening LogChecker.exe

You have chosen to open:

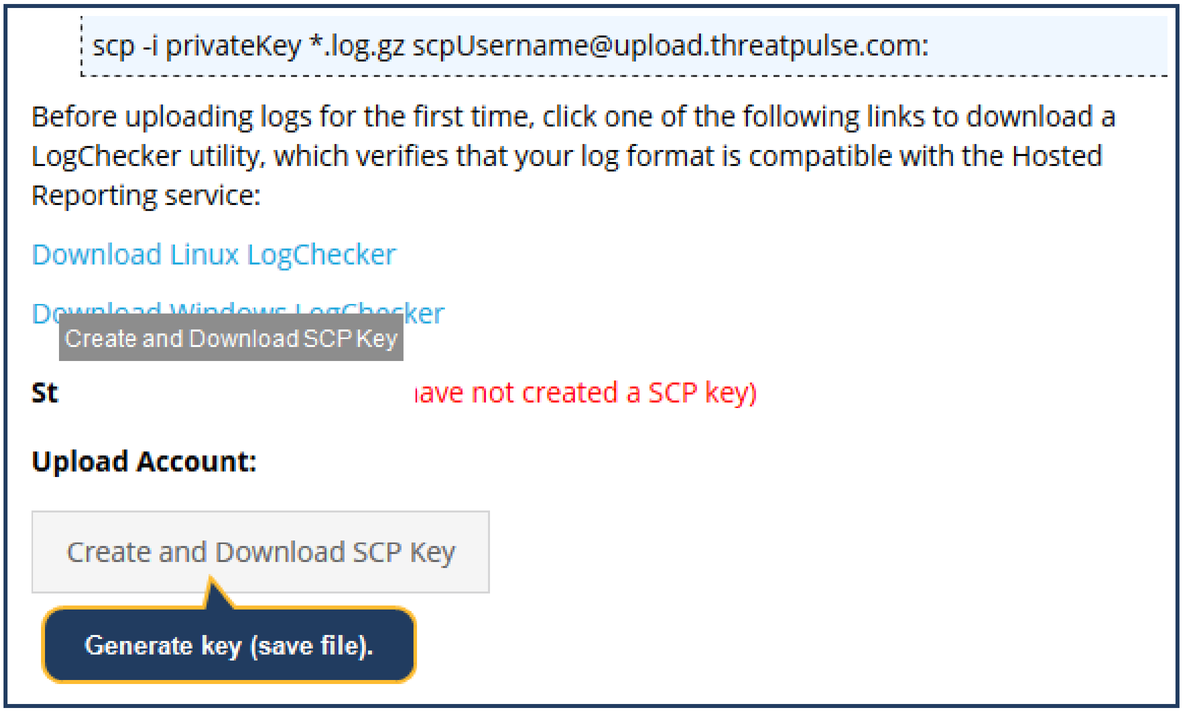
LogChecker.exe

which is: Binary File (128 KB)

from: https://portal.threatpulse.com

Would you like to save this file?

4. Click **Create and Download SCP Key**. This saves a text file that contains your Digital Signature Algorithm (DSA) private key.



```
scp -i privateKey *.log.gz scpUsername@upload.threatpulse.com:
```

Before uploading logs for the first time, click one of the following links to download a LogChecker utility, which verifies that your log format is compatible with the Hosted Reporting service:

Download Linux LogChecker

Download Windows LogChecker

St ave not created a SCP key)

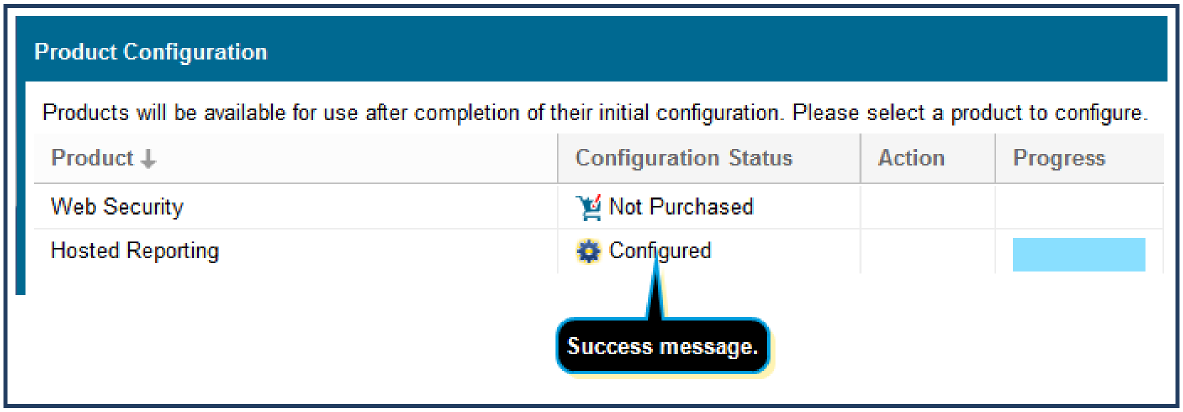
Upload Account:

Generate key (save file).

Save the text file to the same server that contains the access logs.

> **Tip:** The browser you are using might default the file type to something other than a text file. For example, Firefox might default to a comma-separated view (CSV) format file. Before saving the file, verify that it is saving as a text file.

5. Click the **Go Back To Product Setup** button in the lower-right corner.
6. That completes the Initial Configuration process.



Product Configuration

Products will be available for use after completion of their initial configuration. Please select a product to configure.

Product ↓	Configuration Status	Action	Progress
Web Security	Not Purchased		
Hosted Reporting	Configured		

Success message.

To enter the Web Security Service portal, click **Continue**.

> **Tip:** For future reference or needs, your custom `scp` key is viewable on the Service Mode > **Reporting > Hosted Reporting** tab.

Next Step

Verify and upload the main format access logs to an FTP or HTTP staging server. See "Send ProxySG Appliance Access Logs to Staging Server" on the facing page.

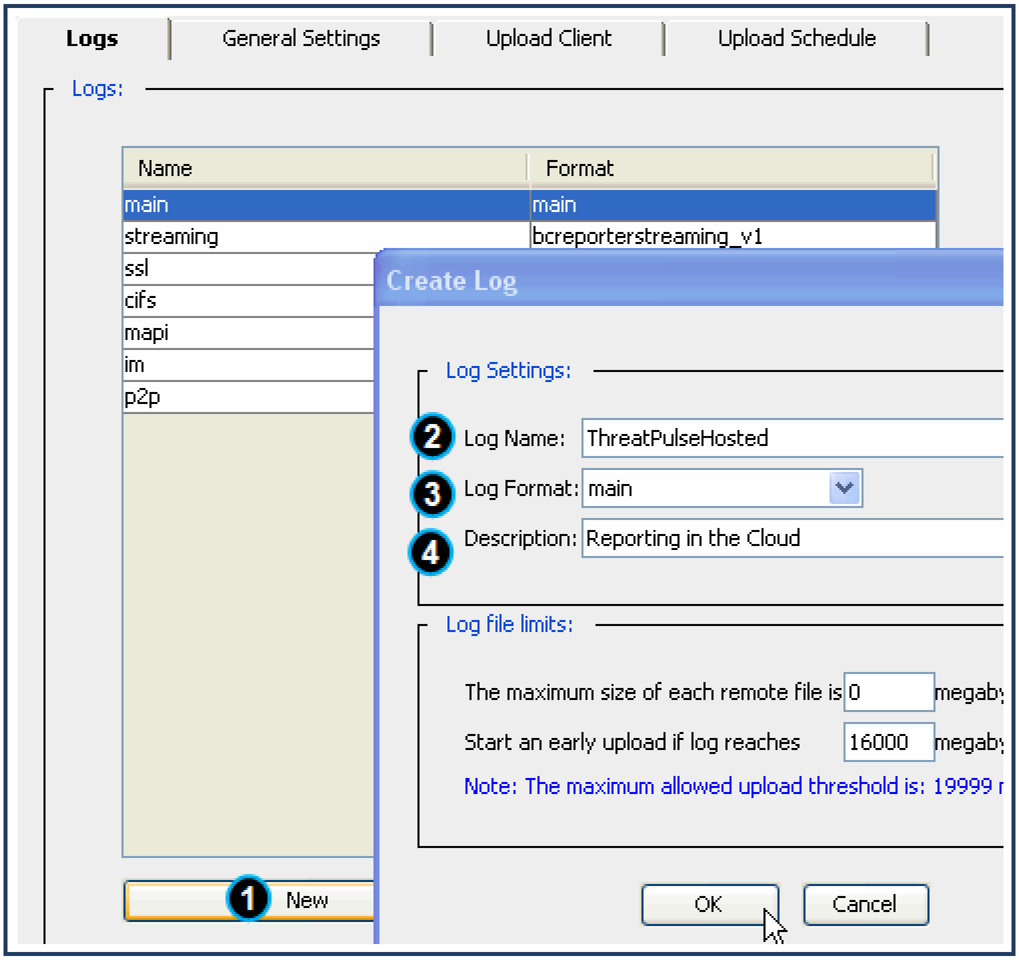
Send ProxySG Appliance Access Logs to Staging Server

After completing the Hosted Reporting Initial Configuration Wizard, (see "Initial Hosted Reporting Configuration" on page 11), the next step is configure the gateway ProxySG appliance log upload client to send its access logs to an FTP or HTTP staging server. This server (Windows or Linux) must have Internet access because the next step involves sending the logs from this server up to the Symantec Web Security Service.

> **Note:** The following procedure references the Proxy Edition SGOS 6.2.x Management Console. Other editions or OS version might slightly differ.

Step 1—Create a main log format for the Web Security Service.

From the ProxySG Management Console, select the **Configuration > Access Logs > Logs > Logs** tab.



Name	Format
main	main
streaming	bcreporterstreaming_v1
ssl	
cifs	
mapi	
im	
p2p	

Log Name: ThreatPulseHosted

Log Format: main

Description: Reporting in the Cloud

The maximum size of each remote file is 0 megaby

Start an early upload if log reaches 16000 megaby

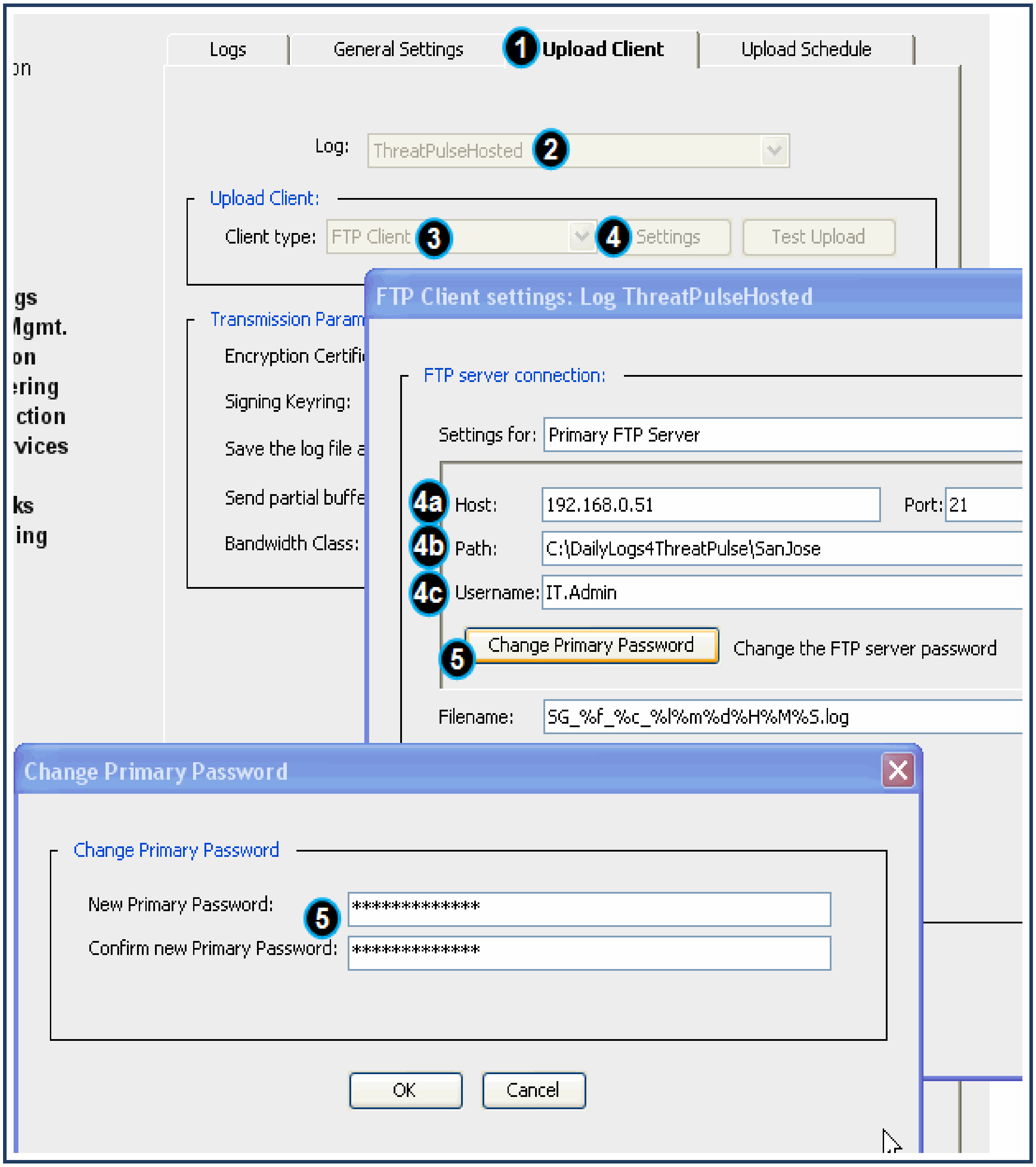
Note: The maximum allowed upload threshold is: 19999 r

1. Click **New**. The device displays the Create Log dialog.
2. **Name** the log. For example, **ThreatPulse Hosted**.
3. From the **Log Format** drop-down, select main.
4. (Optional) Provide a **Description**.

5. Click **OK** to close the dialog.
6. Click **Apply**.

Step 2—Configure the ProxySG appliance upload client to send logs to a staging Windows or Linux FTP or HTTP server.

This example uses FTP.



Log: ThreatPulseHosted

Client type: FTP Client

Settings for: Primary FTP Server

Host: 192.168.0.51 Port: 21

Path: C:\DailyLogs4ThreatPulse\SanJose

Username: IT.Admin

Filename: SG_%f_%c_%l%m%d%H%M%S.log

New Primary Password: *************

Confirm new Primary Password: *************

1. Select the **Configuration > Access Logs > Logs > Upload Client** tab.
2. From the **Log** drop-down list, select the log that you created in **Step 1**.
3. From the **Client Type** drop-down list, select an upload method. This example uses **FTP Client**.
4. Click **Settings**. The device displays the FTP Client Settings dialog.

a. Enter the FTP server **Host** IP address.

b. Enter the **Path** on the server to where the logs are staged. Using location names as folder names helps you differentiate locations. However, this only applies to organizing on the staging server. The Web Security Service does not provided information based that correlates to individual ProxySG appliances.

c. Enter the **Username** required to access the FTP server.

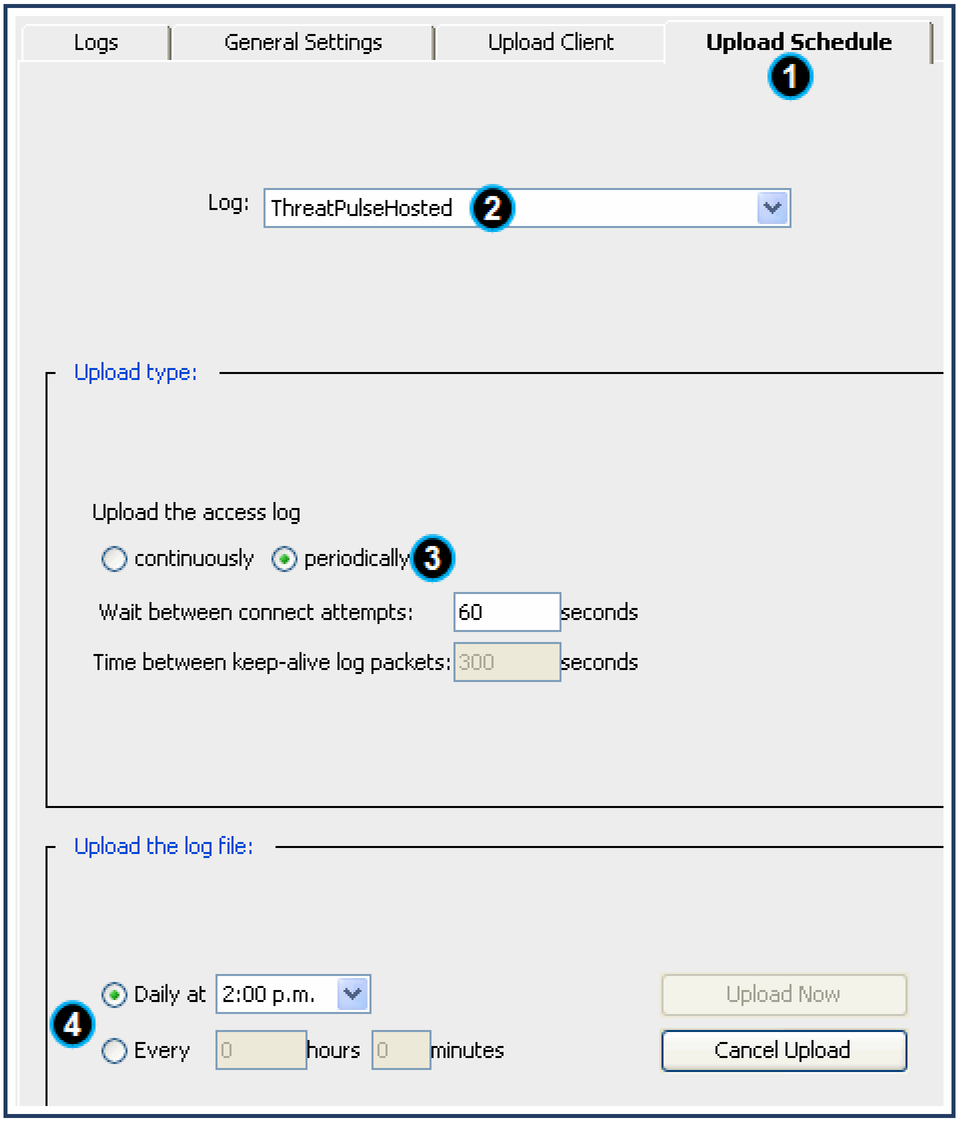
5. Click **Change Primary Password**. The device displays Change Primary Password dialog. Enter the password required to access the FTP server.

6. Click **OK** in each dialog to close.

7. Click **Apply**.

Step 3—Specify the upload schedule for Web Security Service processing.

When planning this, consider that the Web Security Service checks your account every hour for new access logs that were secure-copied from the staging server (described in the next step of this solution). You determine how often the ProxySG appliance sends logs to the staging server. You might elect to send them once a day or every hour for more frequent data processing and current report viewing.



Log: ThreatPulseHosted

Upload type:

Upload the access log

○ continuously ● periodically

Wait between connect attempts: 60 seconds

Time between keep-alive log packets: 300 seconds

Upload the log file:

● Daily at 2:00 p.m.

○ Every 0 hours 0 minutes

1. Select the **Configuration > Access Logs > Logs > Upload Schedule** tab.
2. From the **Log** drop-down, select the log that you created in **Step 1**.
3. Select **Periodically**.
4. Specify the upload schedule. For example, send once **Daily** or **Every** hour.
5. Click **Apply**.

Next Step

Verify log compatibility and secure copy (scp) the logs up to the Web Security Service. See "Secure Copy Access Logs to the Web Security Service" below.

Secure Copy Access Logs to the Web Security Service

After you configure the ProxySG appliance to upload logs to a staging server, the next step is copy them up to your Symantec Web Security Service account. First, run the **LogChecker** application that you downloaded during the Initial Configuration Wizard task (see "Initial Hosted Reporting Configuration" on page 11).

Prerequisite—Verify that the log formats are compatible with the Web Security Service.

Run the **LogChecker** application that you downloaded during the Initial Configuration Wizard task (see "Initial Hosted Reporting Configuration" on page 11).

1. On the Linux or Windows staging server containing the logs, navigate to the folder where you downloaded the **LogChecker** application.
2. Double-click the **LogChecker** program to launch it. The program searches for files with the proper extension.
   - If the test passes, proceed the next section.
   - If the test fails, you must return to your gateway ProxySG appliance deployment and ensure that you are forwarding the access logs in the main format.

     The logs must contain the following fields.

     - Required Fields
       - `date`
       - `time`
       - `cs-host`
       - `cs(Referer)`
       - `sc-status`
       - `cs-uri-scheme`
     - Recommended Fields
       - `c-ip`
       - `cs-username`
       - `x-exception-id`

- `cs-categories`
- `s-action`
- `rs(Content-Type)`
- `cs-uri-path`
- cs-uri-query
- `x-virus-id`

Step 1—Linux Option: Secure copy the log files.

1. Access the command line.
2. Navigate to the folder/directory that contains the logs.
3. Enter the following command, which you copied/recorded during the initial configuration task:

   ```
   scp -i privateKey *.log.gz scpUsername@upload.threatpulse.com:
   ```

   where *scpUsername* is a unique customer identification value provisioned to you by Symantec (**customer*###***).

Step 1—Windows Option: Secure copy the log files.

To use a Windows scp client, you must modify the **privateKey** file. If you do not have the PuTTYgen and PSCP tools, download them here: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

1. Modify the key:
   a. Launch the PuTTYgen tool.
   b. Select **File > Load Key**.
   c. In the dialog, navigate to the saved key location and open it.
   d. Save the private key.
2. Copy the files:
   a. Launch a command prompt window.
   b. Enter the following command, which you copied/recorded during the initial configuration task:

      ```
      pscp.exe -i privateKey *.log.gz scpUsername@upload.threatpulse.com:
      ```

      where *scpUsername* is a unique customer identification value provisioned to you by Symantec (**customer*###***).

Step 2—Post-upload Tasks

To avoid duplicate data in reports, remove the logs from the staging server before uploading new logs because the Web Security Service cannot distinguish between previously processed log files and new ones. As the Web Security Service currently checks for new data every hour, you can write a script to move the current logs before the next ProxySG appliance upload occurs.

Next Step

After the next processing window, generate reports. See "Access the Web Security Service Hosted Reporting Interface" on the facing page.

Access the Web Security Service Hosted Reporting Interface

After you secure copy the access logs to your Web Security Service account, log in to view dashboards, generate reports, define roles, and manage the service.

1. The Web Security Service displays the **Overview** dashboard in Solutions Mode; various report summaries display on the Dashboard.

   > **Tip:** The service processes hosted log files every day at midnight (00:00) UTC time. If you do not see any data, wait until after the next processing window.

2. To learn more about the dashboard, see "What Can I Do From a Hosted Reporting Dashboard?" on page 28.
3. To learn more about reports, see "What Can I Do With Reports?" on page 32

Specify Access Log Retention Duration

Depending on the product, the Symantec Web Security Service retains accumulated access log and report database data that spans a finite number of days or years.

- Web Security: 100 days.
- Hosted Reporting: 1 year.

You might have a personal concern or a corporate edict on how long user data should remain in *the cloud*. The Web Security Service allows you set a limit for how long stored data remains in the reporting database. Before setting the limit, consider the following warning and best practice.

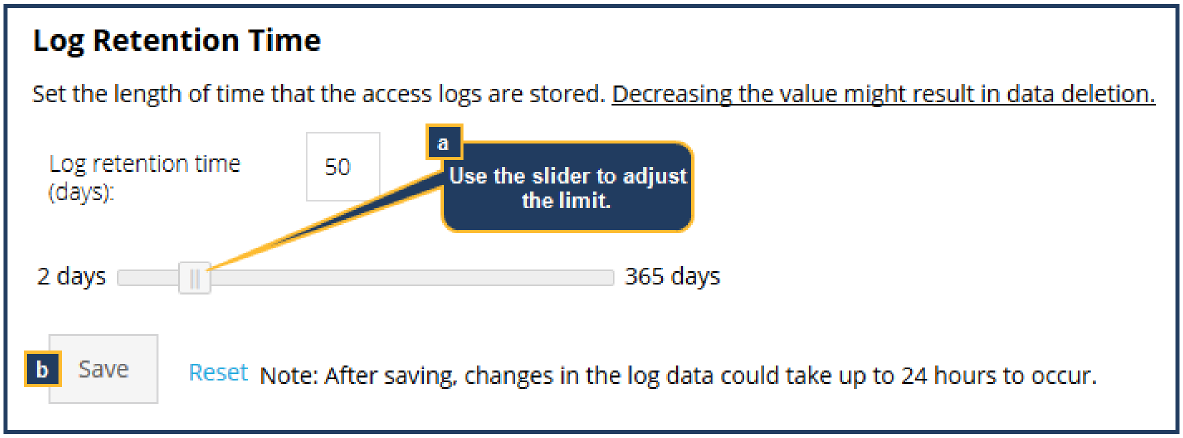
- Reducing a current limit forces the web to purge all older-than-the limit data (chunked in days). You cannot generate reports from the expired data nor can you restore data following a delete action.
- Because of this limitation,Symantec recommends that before you limit retention and expire older data you download the current access logs and archive them. If you have a need to generate more reports from that data, you can re-upload the data; however, consider how the service processes the data.
  - The Web Security Service considers the hardened data as new content; the data remains until the expiration time has passed.
  - The reporter database looks at the log dates. At midnight GMT, the Web Security Service expires that content out again.

  Generate the new reports against the uploaded data as soon as possible.

  To download the access log files, navigate to **Reporting > Log Download**. See "Download Access Logs" on page 24.
- Review any scheduled reports. If you limit the retention to 15 days and you have a report that generates every 30 days, the report will not contain 50% of the user-generated data because the Web Security Service deleted the logs.

Procedure

1. In Service Mode; select **Reporting > Log Retention**.



Log Retention Time

Set the length of time that the access logs are stored. Decreasing the value might result in data deletion.

Log retention time (days): 50

Note: After saving, changes in the log data could take up to 24 hours to occur.

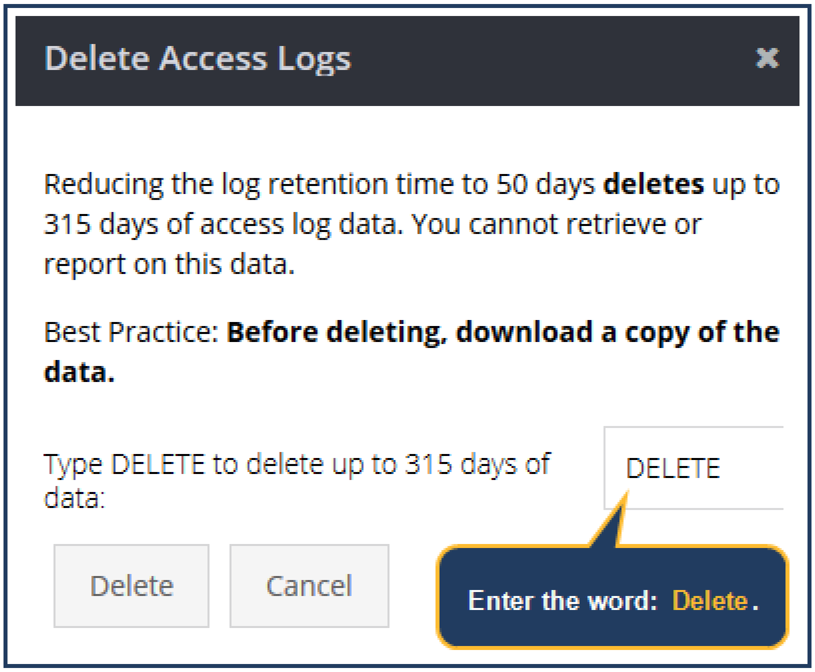
a. Move the slider to adjust the retention limit.

> **Tip:** The initial value varies—100 days to 1 year—depends on the Web Security Service product).

As you move the slider, the **Log Retention Time** fields (the **Log Retention Time** field and the field hovering over the slider) display the limits.

b. When you are satisfied with the limit, click **Save**.

2. For a verification mechanism, the portal displays the Delete Access Logs dialog.



Delete Access Logs

Reducing the log retention time to 50 days **deletes** up to 315 days of access log data. You cannot retrieve or report on this data.

Best Practice: **Before deleting, download a copy of the data.**

Type DELETE to delete up to 315 days of data: DELETE

The dialog reminds you of the log download best practice mentioned above. The dialog also indicates how many days of data the service will delete if you enact the limit. To enact the limit, you must enter the word **DELETE** in the field and click **OK**. If you enter any other characters and click **OK**, the service does *not* enact the limit.

As stated on the screen, the service might require up to 24 hours to adjust to the new limit.

Reset

The **Reset** link on the page moves the limit to the previously set limit *before* you click **Save**. To restore the service default, move the slider fully to the right.

Download Access Logs

As the Symantec Web Security Service processes web traffic requests and transactions, it stores the hourly access logs in the service. The services allows you to download these raw log files as zip files that contains selected one-hour log files or daily log files that contain all 24 one-hour log files. There are two use cases for this:

- For the Web Security ServiceHosted Reporting service, the logs are retained for 100 days in the reporting databaseone year in the reporting database. When this milestone is reached, the Web Security Service begins deleting log file data on a daily basis, beginning with the oldest day. Download the logs for your own archiving purposes.
- You use the Symantec Reporter product and you want to use it to reprocess specific logs. You must use Symantec Reporter **9.x Enterprise Edition** or Symantec Reporter **10.1.5**.

The log files are aggregates of all configured locations that feed into the Web Security Service.

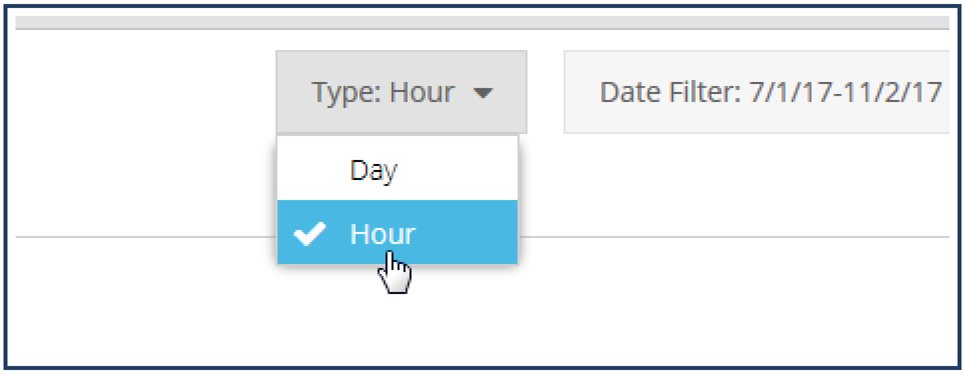
> **Tip:** If you have access to the Hosted Reporting product, you can re-upload the logs back to the Web Security Service. Be advised that the service cannot recognize data it has previous processed. If you upload logs that contain previously processed data, the result is bloated data—that is, the reports display double the previous values. Take care to manage your download log files.

> **Tip:** As a Hosted Reporting user, you can re-upload the logs back to the Web Security Service. Be advised that the service cannot recognize data it has previous processed. If you upload logs that contain previously processed data, the result is bloated data—that is, the reports display double the previous values. Take care to manage your download log files.

Download Raw Access Log Files

In Service Mode, select **Reporting > Log Download**.

By default, the portal lists the log files by **Day** in the order that the *service receives* them beginning with the oldest date (in UTC). The service display ten days per page. To view more selectable days, click the arrow keys in the footer.



a. If necessary, select a **Date Filter** (select the **Start Date** and **End Date**, which correspond to the date range of the received logs, not necessarily the dates of the actual Web transactions).

b. (Optional) Change the view by selecting **Hour** from the **Type** drop-down.

c. Select the files on displays pages; you *cannot* select files across multiple pages.

d. Click **Download**.

e. Given your browser vendor, the zip download/open dialog displays or the zip download displays (for example, in Chrome). **Save the File** to a staging or archive server or directly to the Reporter 9.x server or 10.1.5+ appliance, if using that option (see next section).

For Use With Symantec Reporter 9.x or 10.1.5+

The zip file contains `*.log.gz` files. Each one of those files represents an hour (received timestamp) of data. and can be directly imported into Reporter. To use Reporter to process raw Web Security Service log files, Symantec recommends the following steps:

1. Save or FTP the raw access logs to the server from which Reporter is configured to process. Consider creating folder names that identifies the files; for example, **`Cloud_Archive`**.
2. In Reporter, create a new database (**Administration**: **General Settings > Reporter Settings > Data Settings > Databases**).
3. Set the **Log Source** as the folder you created for the Web Security Service logs.

Scenarios That Require New SCP Keys

Forwarding ProxySG appliance access log files to the Symantec Web Security Service for reporting requires you to generate a digital security algorithm (DSA) key that is used during the secure copy (scp) process. You create and download this during the configuration process as described in "Initial Hosted Reporting Configuration" on page 11.

Some circumstances might require you to recreate this key. They include:

- Your company security best practices require you to frequently change encryption keys.
- You misplaced or deleted the original key file.

To recreate a new key:

1. In Service Mode, select **Reporting > Hosted Reporting**.
2. Click **Create and Download SCP Key**.
3. Save the key on the access logging staging server.

About Reporting

The section how to manage the Web Security Service reports.

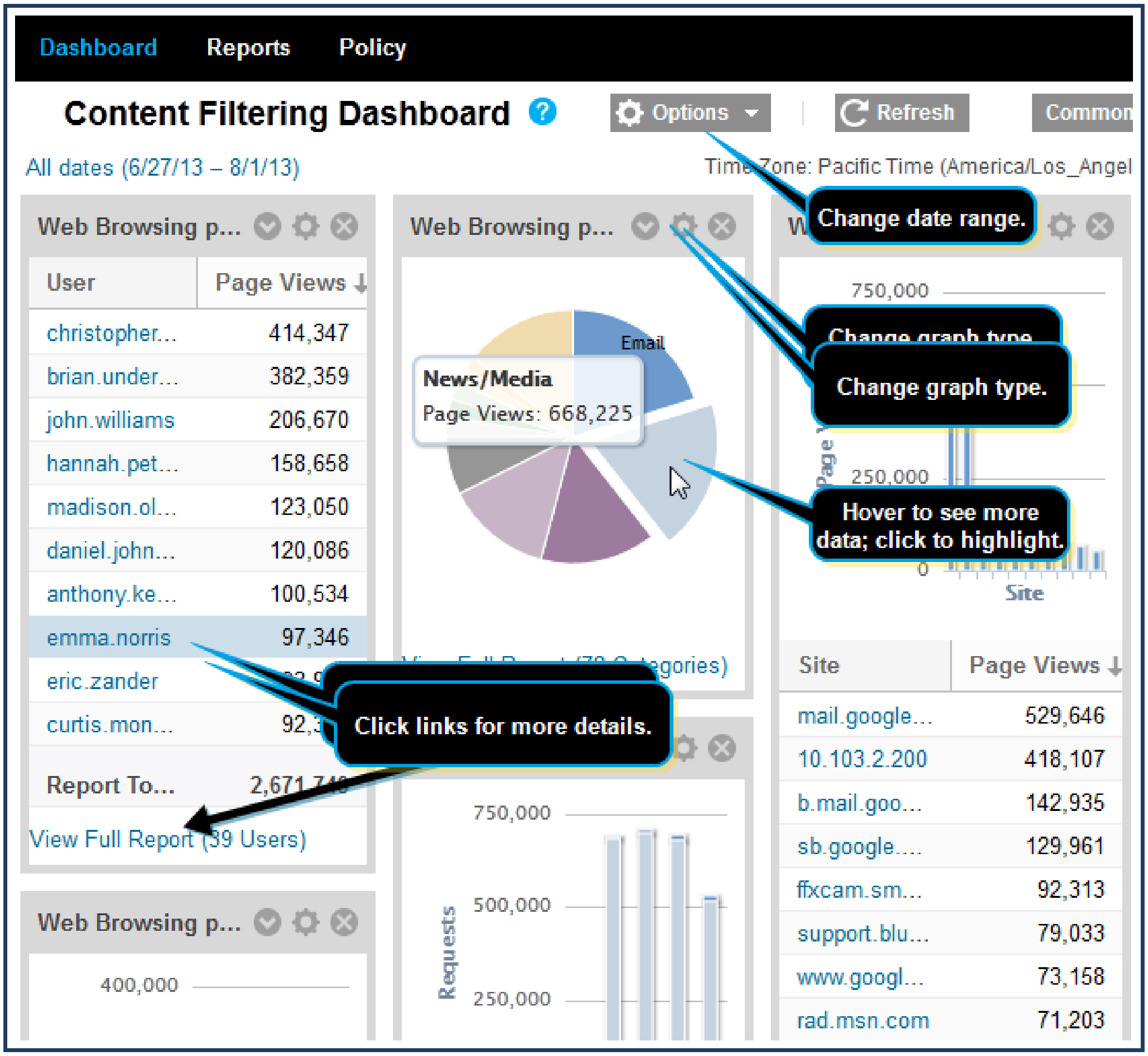
What Can I Do From a Hosted Reporting Dashboard?

Each Symantec Web Security Service module—**Content Filtering**, **Threat Protection** (malware), and **Search Controls** (Web Application reports and search engine policy)—provides a report Dashboard, which displays high-level summaries of web browsing activities as they apply to the selected module. Additionally, the **Overview** dashboard provides commonly monitored summaries from all modules.

Expand the following sections to learn about Dashboard features.

Analyze Data

Dashboards present data in graphs and/or tables. You can change the date range (for the entire dashboard view), change the graphic style for each report widget, and rollover or click report elements to view more details.



All dates (6/27/13 – 8/1/13)

Time Zone: Pacific Time (America/Los_Angel

Change date range.

Change graph type.

Change graph type.

Hover to see more data; click to highlight.

Click links for more details.

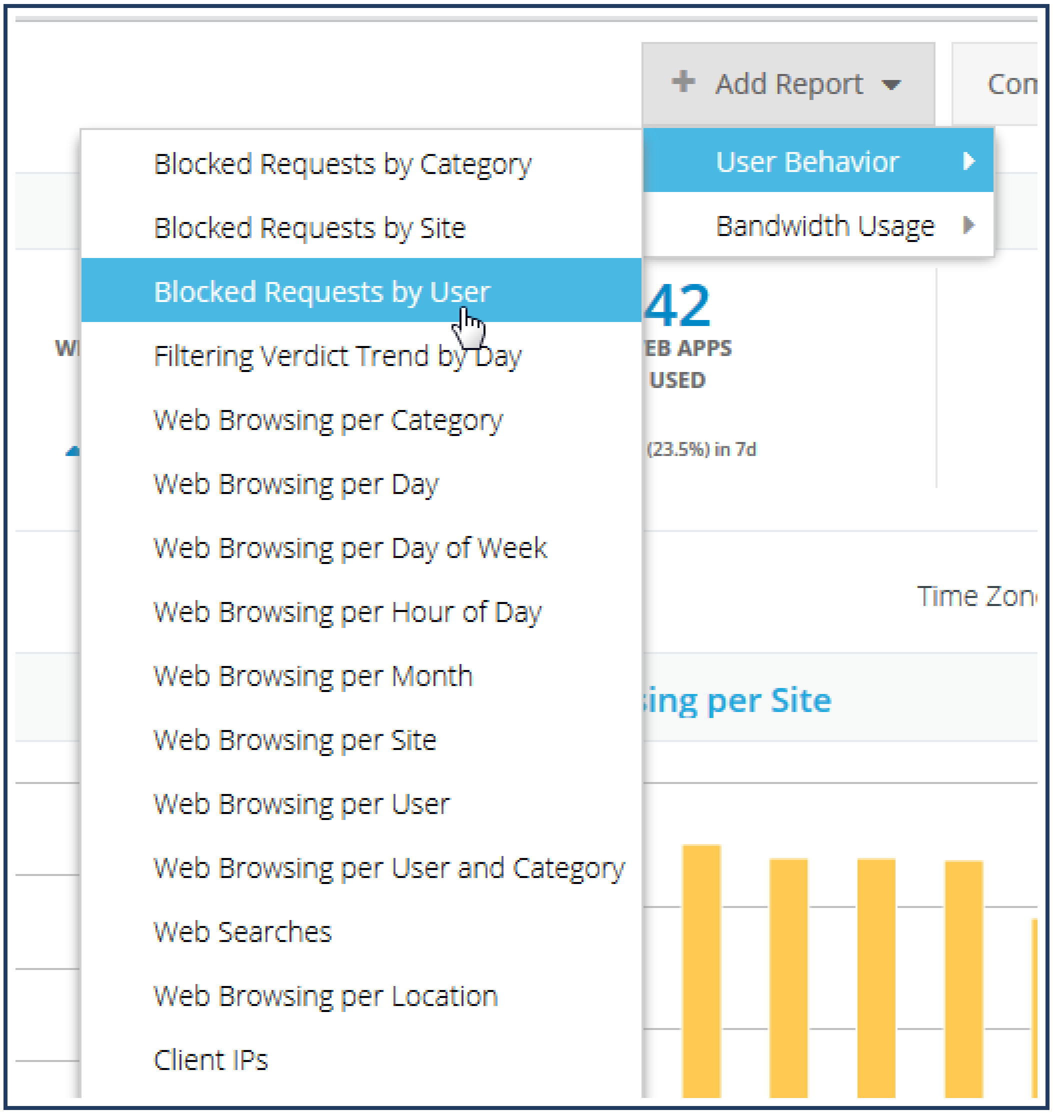
User	Page Views ↓
christopher...	414,347
brian.under...	382,359
john.williams	206,670
hannah.pet...	158,658
madison.ol...	123,050
daniel.john...	120,086
anthony.ke...	100,534
emma.norris	97,346
eric.zander	92,9
curtis.mon...	92,3
Report To...	2,671,74

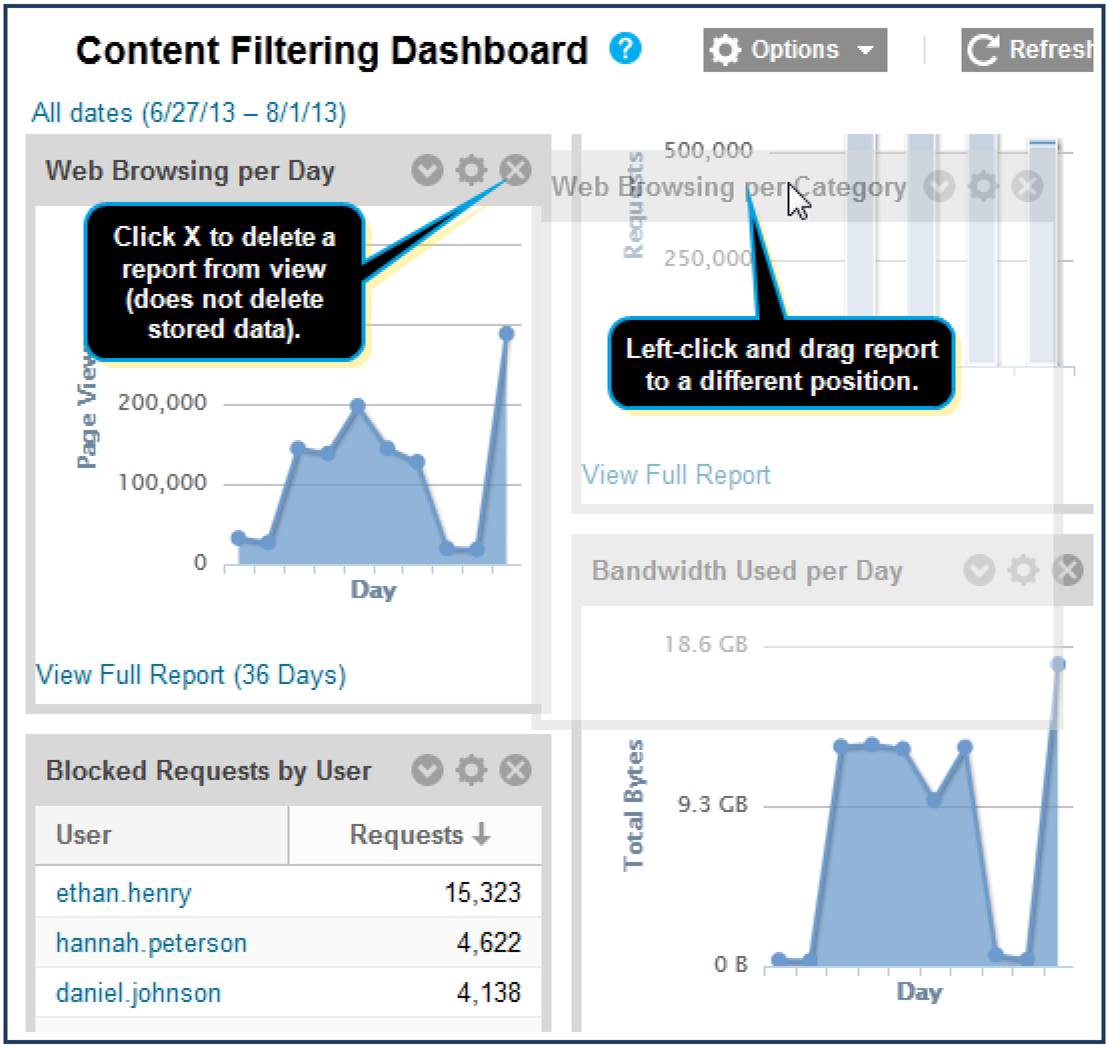
View Full Report (39 Users)

Site	Page Views ↓
mail.google...	529,646
10.103.2.200	418,107
b.mail.goo...	142,935
sb.google....	129,961
ffxcam.sm...	92,313
support.blu...	79,033
www.googl...	73,158
rad.msn.com	71,203

Customize Dashboard View

To display the data most important to your monitoring goals, add, move, or delete summary reports.


+ Add Report
Con
User Behavior
Bandwidth Usage
Blocked Requests by Category
Blocked Requests by Site
Blocked Requests by User
Filtering Verdict Trend by Day
Web Browsing per Category
Web Browsing per Day
Web Browsing per Day of Week
Web Browsing per Hour of Day
Web Browsing per Month
Web Browsing per Site
Web Browsing per User
Web Browsing per User and Category
Web Searches
Web Browsing per Location
Client IPs
42
EB APPS
USED
(23.5%) in 7d
Time Zon
ing per Site



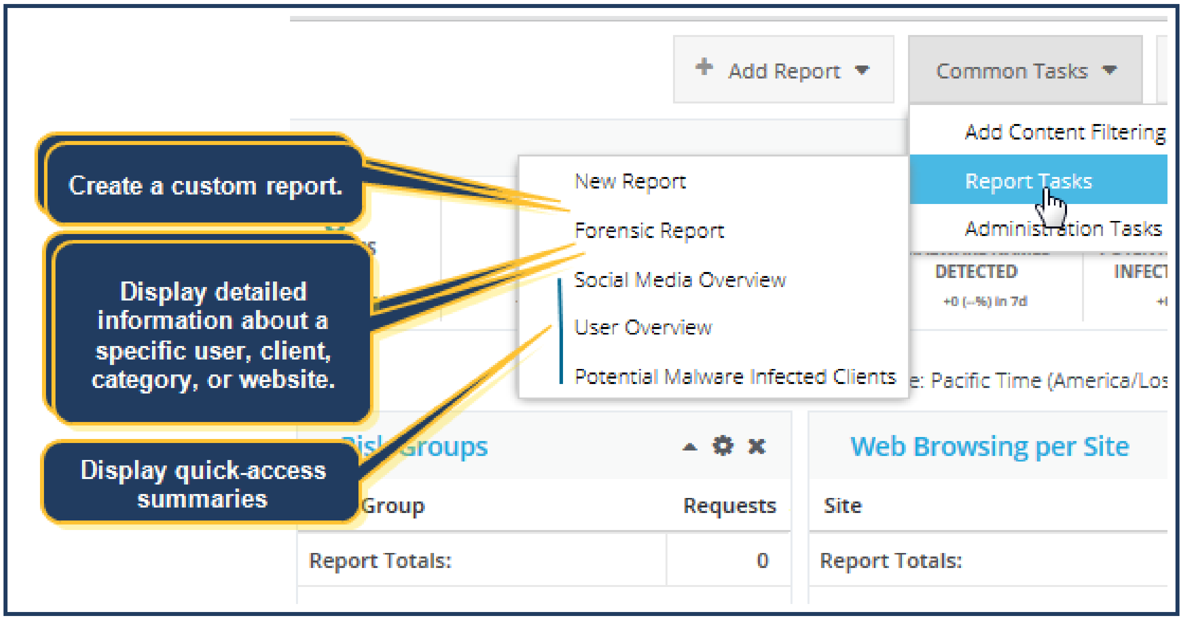
Click X to delete a report from view (does not delete stored data).

Left-click and drag report to a different position.

User	Requests ↓
ethan.henry	15,323
hannah.peterson	4,622
daniel.johnson	4,138

Access Other Reports

The upper-right corner of Dashboards contains a drop-down called **Common Tasks**. From this list, navigate to other reporting features. Create a custom report, investigate with a forensic report, and quickly access targeted summaries.



Create a custom report.

Display detailed information about a specific user, client, category, or website.

Display quick-access summaries

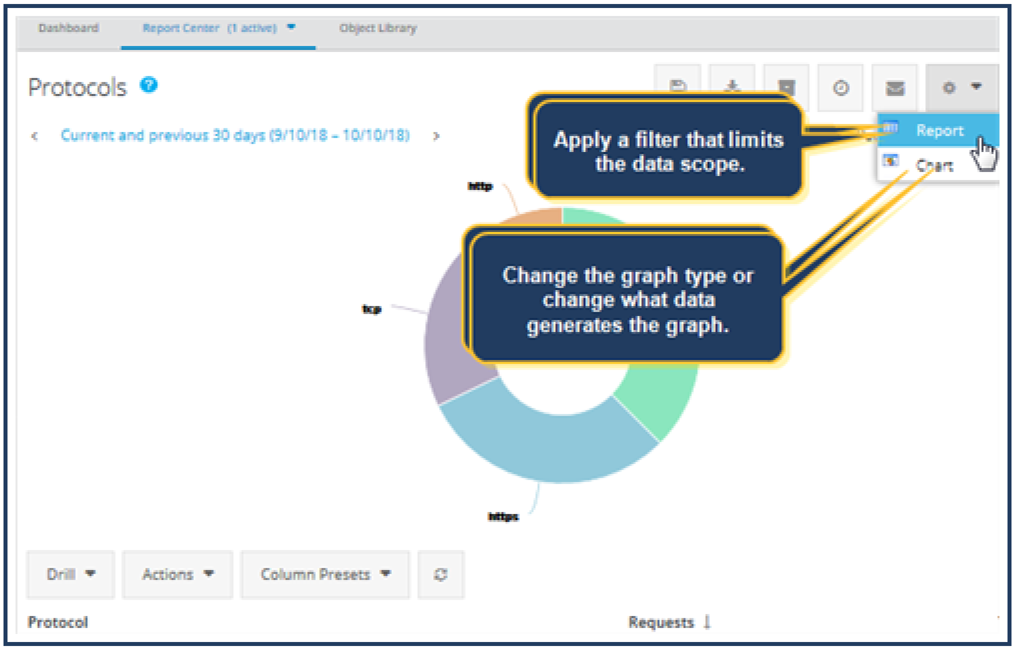
What Can I Do With Reports?

Symantec Web Security Service reports display either information based on pre-defined criteria or custom criteria. Each report contains several features that allow you to manage how reports are analyzed and distributed.

Expand the following sections to learn more about report features.

Change Report

Most predefined reports display results that include a wide scope of data. When reviewing reports results, you can apply filters to limit the scope of the results. Also, when you change the scope of the reports, the default graphic might not best represent the new data set.



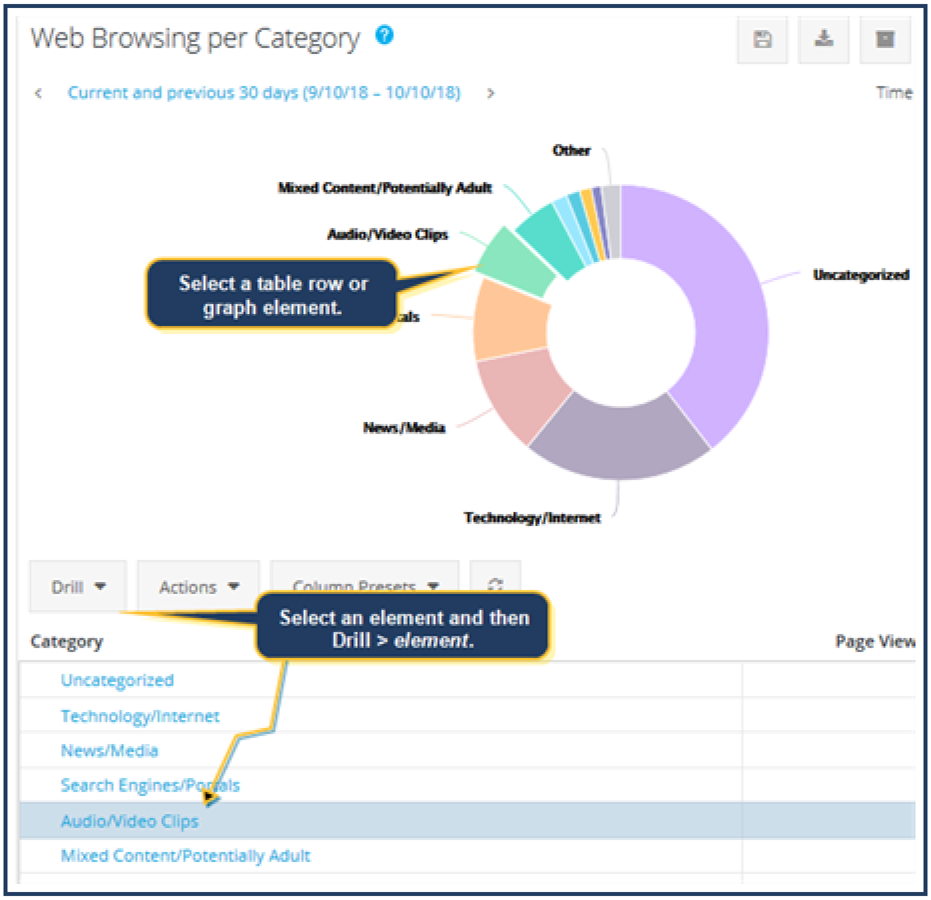
Apply a filter that limits the data scope.

Change the graph type or change what data generates the graph.

View More Details

There are two ways to view more details.

- Select a row and click **Drill**; select an element to view. For example, you want to see which requested sites are known spyware sites.



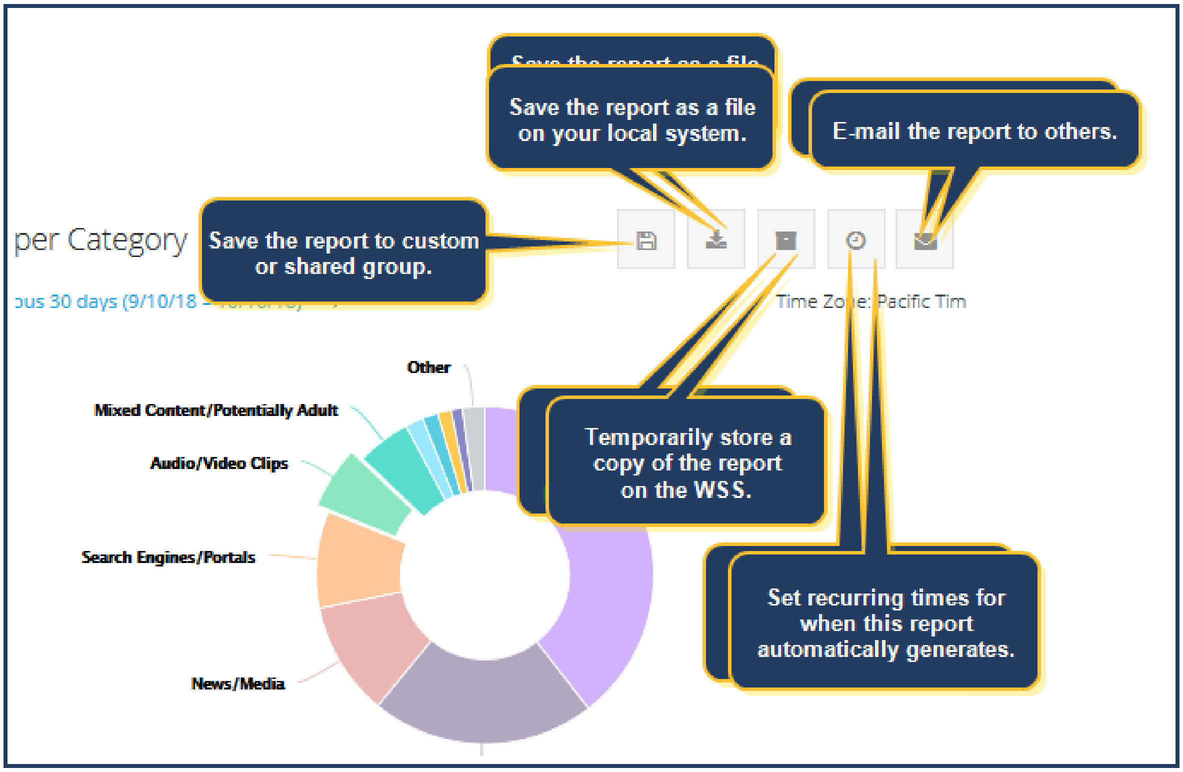
Select a table row or graph element.

Select an element and then Drill > *element.*

- Click any blue link to see more details related to the item, such as who performed requests, site names, applications used, and more. For example, click a user name to see

Manage Reports

Each reports contains options that enable you to schedule automatic generation times, save as a file, and send to others.


per Category
ous 30 days (9/10/18 –
Time Zone: Pacific Tim
Other
Mixed Content/Potentially Adult
Audio/Video Clips
Search Engines/Portals
News/Media
Save the report to custom or shared group.
Save the report as a file on your local system.
E-mail the report to others.
Temporarily store a copy of the report on the WSS.
Set recurring times for when this report automatically generates.

Schedule Report Generation

If personnel in your company are required to see the same Symantec Web Security Service report on a periodic basis, schedule when the reports generate and configure the service to save the file or e-mail it.

You can generate the report in one of three formats:

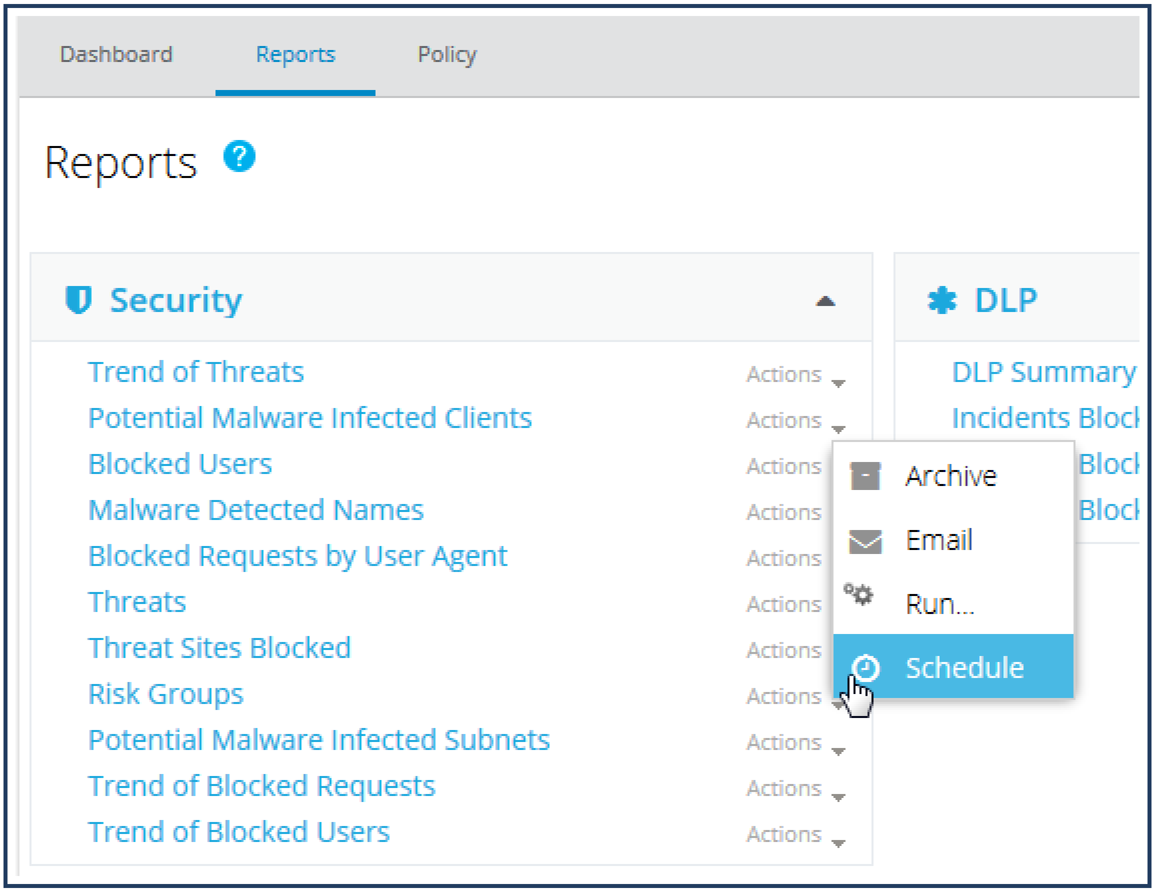
- **PDF**—Opens with Adobe Acrobat/Reader.
- **CSV**—Comma-delineated file that opens with a compatible spreadsheet application (such as Excel).

  > **Tip:** If the generated report begins with incorrect characters—for example: `ï»¿Category`—switch to the **CSV (Raw)** format.

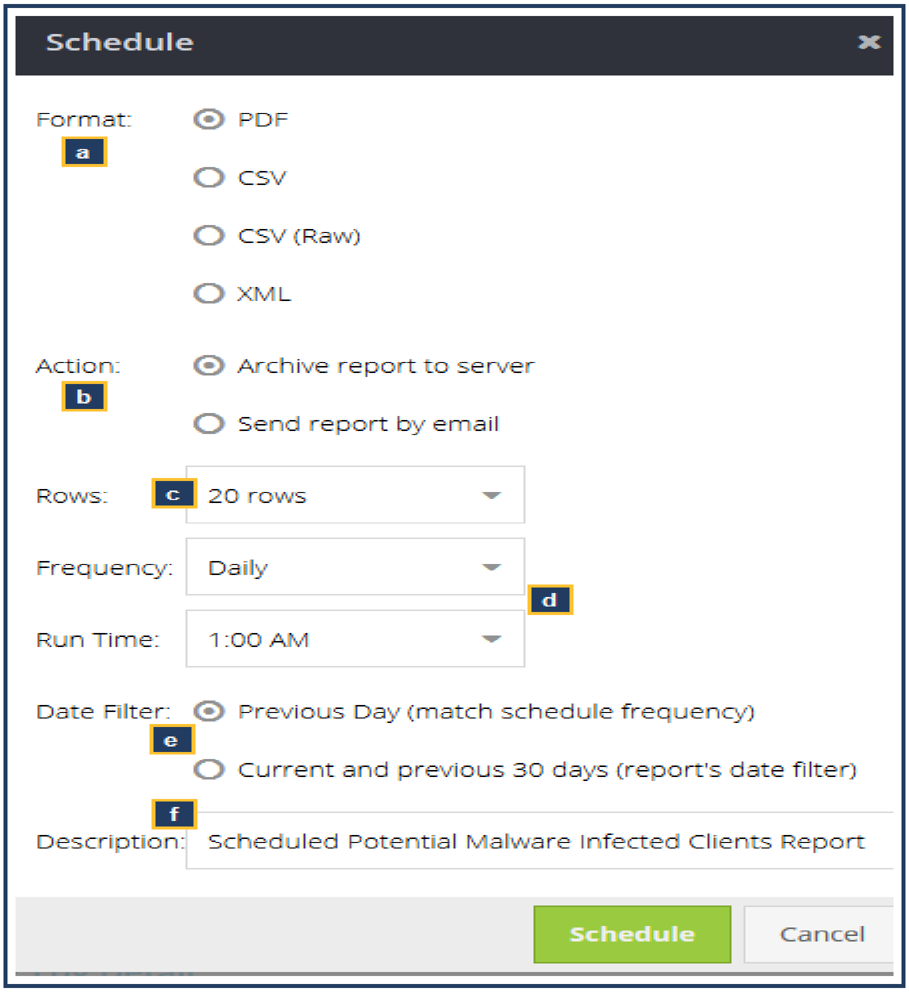
- **XML**—Exports report data in standard XML format to be opened by external applications.

Procedure

1. Click the **Solutions** link.
2. Two locations provide access to the scheduler:
   - Individual report pages—click the **Schedule** icon.
   - The **Report Center** and **Reports** links on the solution tabs—select **Schedule** from the **Actions** drop-down lists.



3. Specify the schedule.



Format: ● PDF ○ CSV ○ CSV (Raw) ○ XML

Action: ● Archive report to server ○ Send report by email

Rows: 20 rows

Frequency: Daily

Run Time: 1:00 AM

Date Filter: ● Previous Day (match schedule frequency) ○ Current and previous 30 days (report's date filter)

Description: Scheduled Potential Malware Infected Clients Report

a. Select the **Format** that the report saves as **PDF**, **CSV** or **CSV (Raw)**, or **XML**.

b. Select the **Action** to take when the report generates:

- **Archive report to server**—The Web Security Service saves the generated report and displays it in the **Recent Archived Reports** area on all **Reports** link tabs.
- **Send report by email**—The Web Security Service generates the report and sends it to the specified recipient(s). This is an effective way to send targeted information to different personnel who are responsible for managing or monitoring specific information.

c. Select the number of **Rows**. If using the **E-mail** action, consider size limitations of the recipient's inbox.

d. Specify when and how often the report generates.

- Select the **Frequency**: **Daily**, **Weekly**, or **Monthly**.
- Select the **Run Time**, which is the hour of the day.
- Select a **Run Day** option to specify on which day, in conjunction with the **Frequency**, the report runs (this option does not display if the **Frequency** is **Daily**).

- If you set the **Frequency** to **Weekly**, select a day of the week.
- If you set the **Frequency** to **Monthly**, select the **First Day** or **Last Day** of the month or a **Custom** day. **Important:** If you select the **Last Day** option, the report runs on the final day of month regardless of the number of days. For example, February 28th or July 31st. If you require a strict 30-day interval for the data, see the next option.

e. Select a **Date Filter**. The **Previous** option changes to match the **Frequency** selection. The **All dates** option generates the report using the date filter that is applied to that report.

f. Accept the default **Description** or enter a custom one.

g. Click **Schedule**.

Archive Report Results

As you generate and review Symantec Web Security Service reports, you might decide to save the report results on the system and return to the file at a later time. For example, you are generating several reports types and will determine which one is the more relative to forward at the conclusion of your analysis.

You can save the archived report in one of three formats:

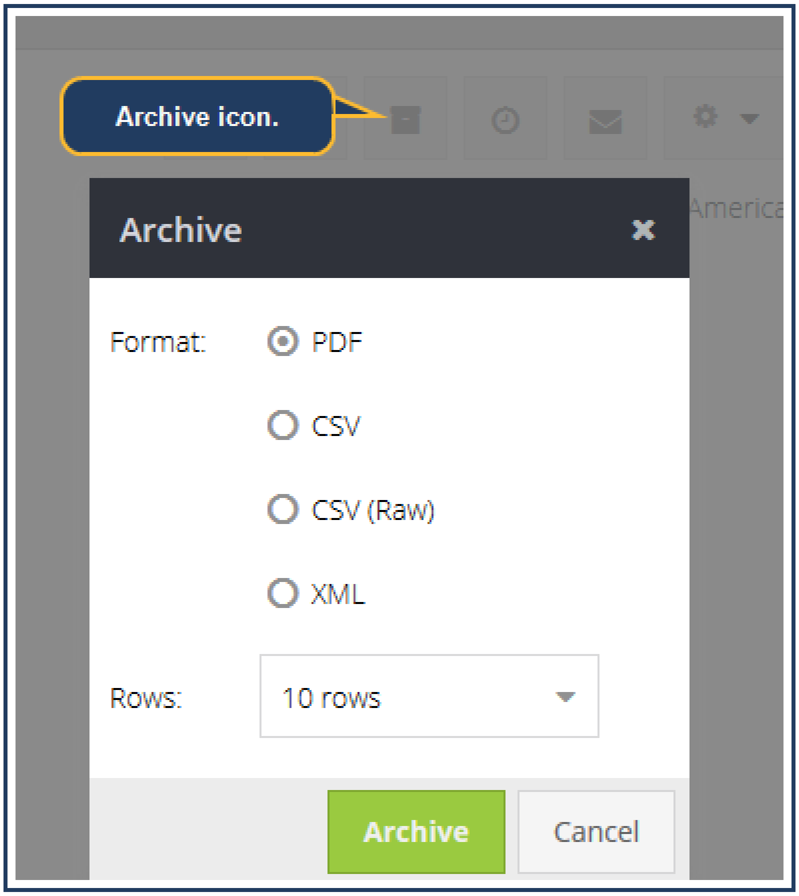
- **PDF**—Opens with Adobe Acrobat/Reader.
- **CSV**—Comma-delineated file that opens with a compatible spreadsheet application (such as Excel).

> **Tip:** If the generated report begins with incorrect characters—for example: `ï»¿Category`—switch to the **CSV (Raw)** format.

- **XML**—Exports report data in standard XML format to be opened by external applications.

Archive Procedure

1. In Solutions Mode, generate any report.
2. In the upper-right corner, click **Archive**. The portal displays the Archive dialog.



Archive icon.

Archive

Format: ◉ PDF

○ CSV

○ CSV (Raw)

○ XML

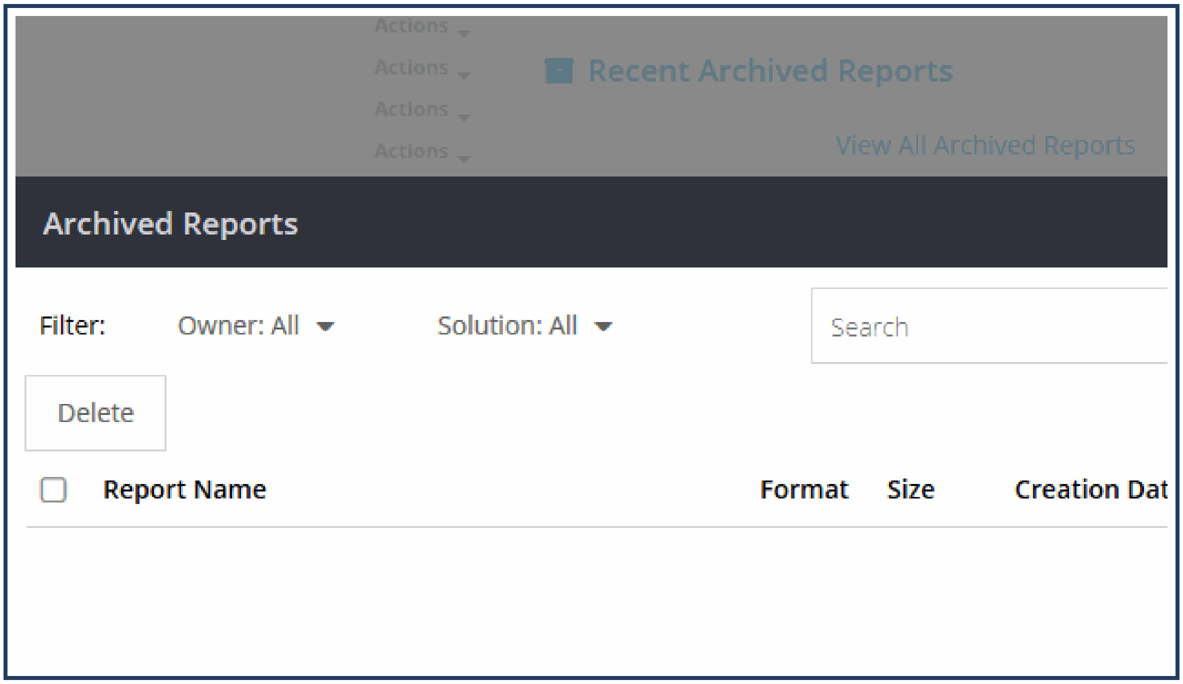
Rows: 10 rows

   a. Select the report **Format**.

b. Specify how many **Rows** the report displays. For example, you are only concerned with the top **20** results.

c. Click **Archive**. The Web Security Service generates the report in the selected file format.

The portal displays the report in the **Recent Archived Reports** area on the **Reports** link. Click the View All Archived Reports Link to display a dialog in which you can navigate these reports.



From here, you have the option sort by process, to **Delete** the report, **Download** the report for yourself or to send to others, or **View** the report in the saved format (requires Adobe Acrobat/Reader, a spreadsheet application, or an application that reads XML).

E-mail a Report

The Symantec Web Security Service allows you to e-mail a copy of any report to one or more recipients. For example, you notice an unusual spike in a particular traffic type and you want to inform others in your organization.

You can e-mail the report in one of three formats:

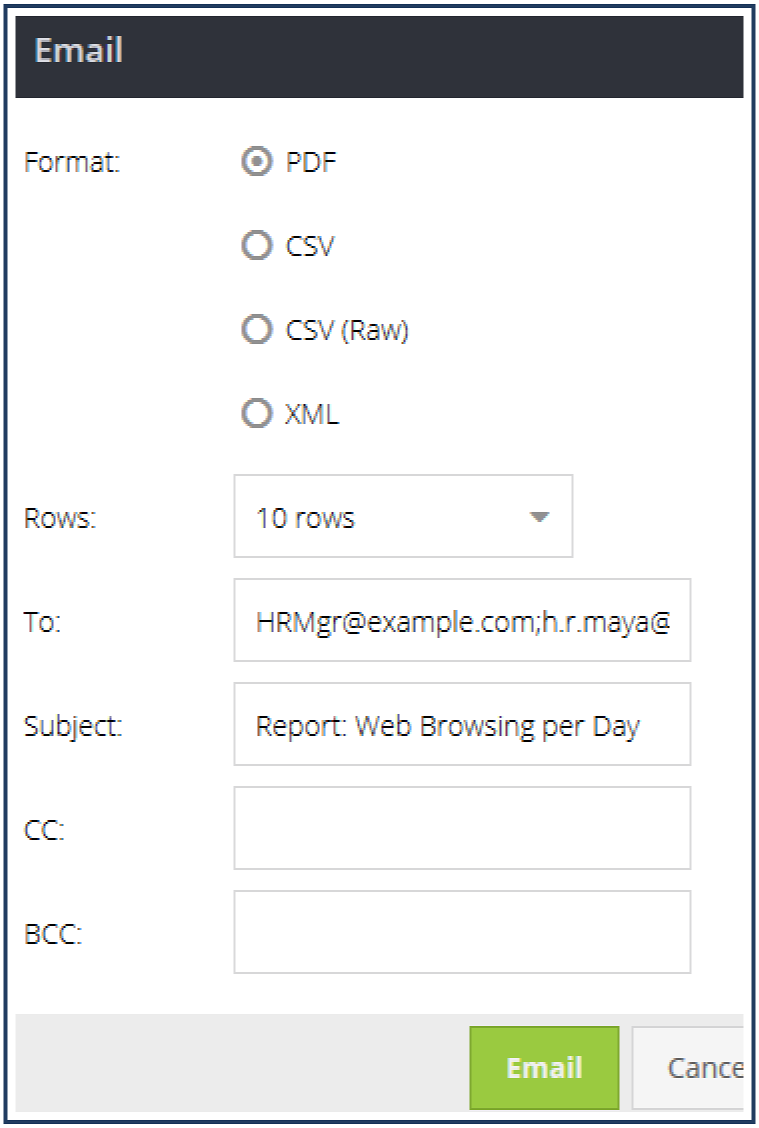
- **PDF**—Opens with Adobe Acrobat/Reader.
- **CSV**—Comma-delineated file that opens with a compatible spreadsheet application (such as Excel).

> **Tip:** If the generated report begins with incorrect characters—for example: `ï»¿Category`—switch to the **CSV (Raw)** format.

- **XML**—Exports report data in standard XML format to be opened by external applications.

Procedure

1. In Solutions Mode, generate any report.
2. In the upper-right corner, click **Email**. The Email dialog displays.



Email

Format: ● PDF ○ CSV ○ CSV (Raw) ○ XML

Rows: 10 rows

To: HRMgr@example.com;h.r.maya@

Subject: Report: Web Browsing per Day

CC:

BCC:

a. Select the report **Format**.

b. Specify how many **Rows** the report displays. For example, you only want to send the top **10** results.

c. Enter **To** whom receives the e-mail. Enter commas to separate multiple recipients.

d. The default **Subject** is the title of the report. Accept the default or add/replace text. For example, `Requires immediate attention: social media traffic spike`.

e. Click **Email**.

Examine Detailed User or Client Activity

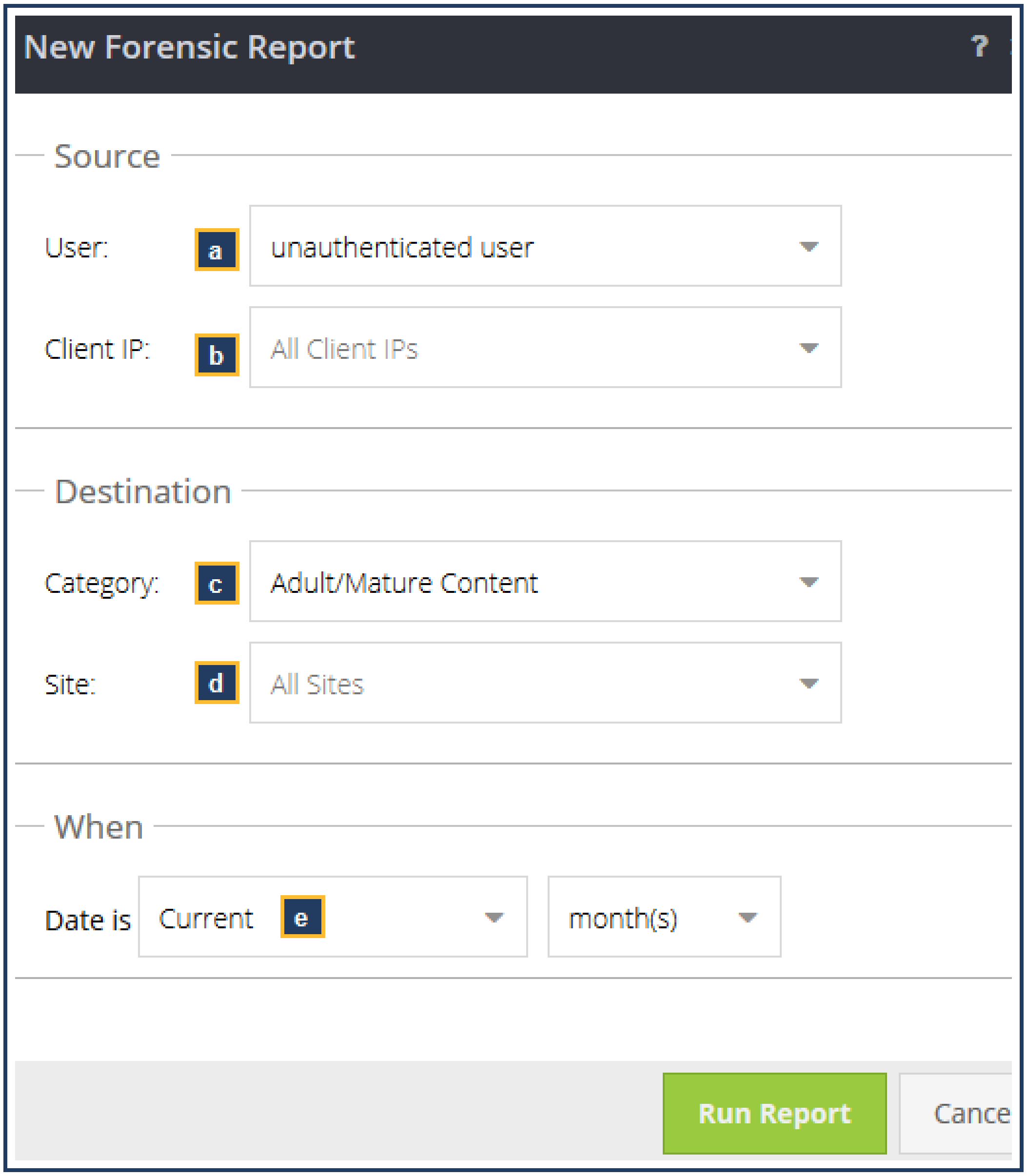
The Symantec Web Security Service provides a *forensic report* option that displays information about a specific user, client, category, or website.

Use Cases

- Someone at your company observed a visiting vendor, who was logged into your guest network, browsing offensive web locations. You want to run a report for that day so you can forward it to the vendor and ask that future visitors refrain from such activity.
- You suspect a particular client is infected with malware and you want to see a detailed report for all activity as it relates to that client.
- You want a browsing behavior breakdown for one specific user.

Procedure

1. In Solutions Mode, two locations provide access to the Forensic Report:
   - Any **Dashboard** link, select **Common Tasks > Report Tasks > Forensic Report**.
   - The **Overview > Report Center** page, click **Forensic Report**.
   - Any **Reports** link, click **Forensic Report**.
2. In the New Forensic Report dialog, enter the generation criteria. You can select any or all of the options.



New Forensic Report

Source

User: unauthenticated user

Client IP: All Client IPs

Destination

Category: Adult/Mature Content

Site: All Sites

When

Date is Current month(s)

a. Select a **User**; if you know the username, begin typing to use auto-fill. This examples looks for **unauthenticated users**.

b. To restrict the report to a single client, select or enter a **Client IP**.

c. To restrict the report to single **Category**, select or enter one. This example displays results for unauthenticated users who browsed **Adult/Mature Content** sites.

d. To restrict the report to a known destination **Site**, select or enter one.

e. To specify a time frame of user activity, select a **Date is** option. This example uses the **Custom** option and isolates the day when the visitor was on campus.

f. Click **Run Report**.

Using the specified criteria, the Web Security Service generates and displays **The Full Log Detail** report.

- If the report does not display the desired data set, select **Reports > Close Current** and repeat the procedure with other search criteria.
- If the report satisfies your needs, save and disperse as required. See "What Can I Do With Reports?" on page 32.

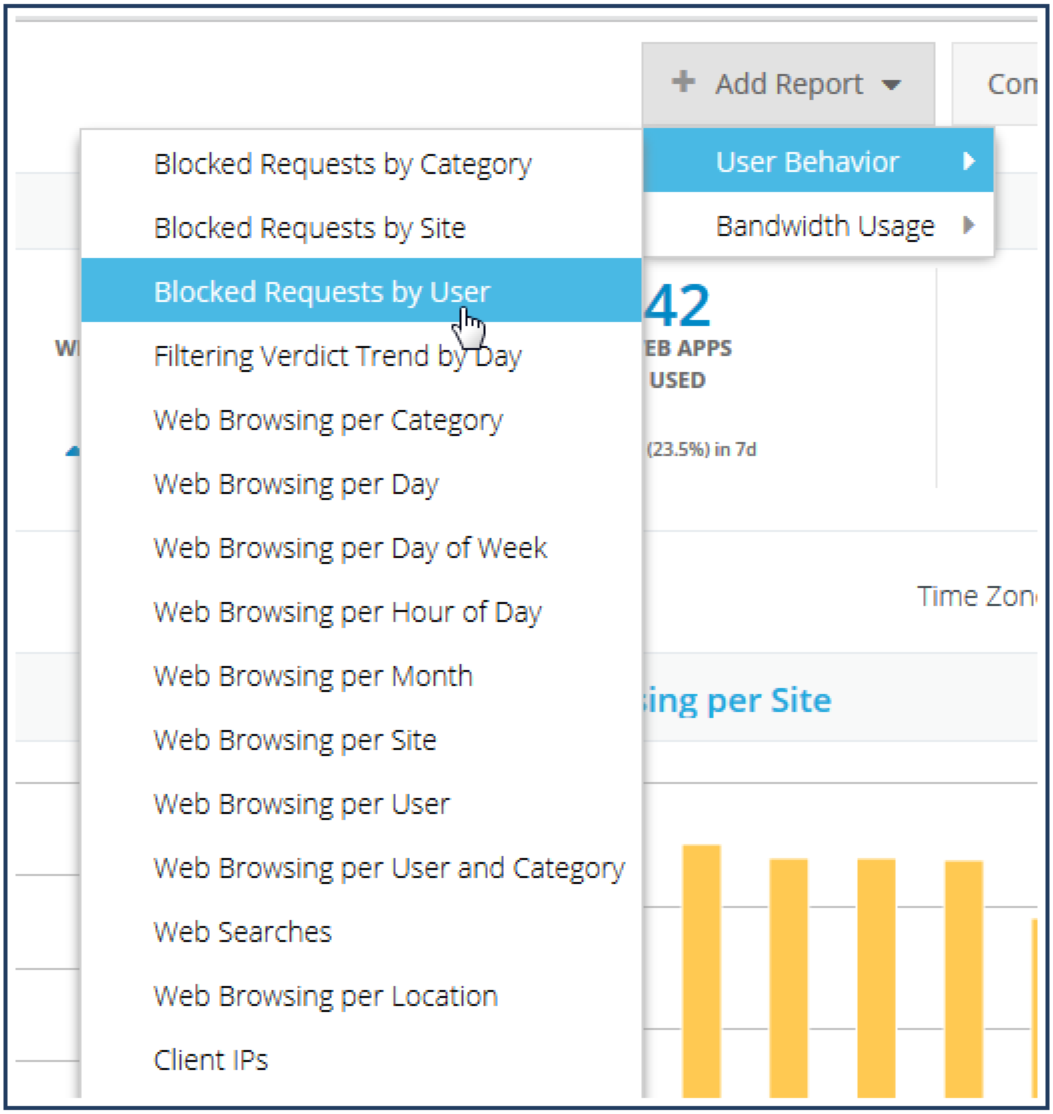
Add a Report to a Web Security Service Dashboard

Each Symantec Web Security Service modules—**Content Filtering**, **Threat Protection**, **and Search Controls** —provide report Dashboards. Additionally, the **Overview** dashboard provides commonly monitored summaries from all modules. Each Dashboard displays its own set of default reports, which are high-level summaries. To customize your Dashboard view, add other reports.

1. Access any Dashboard—**Content Filtering**, **Threat Protection**, or **Overview**.

> **Tip:** The **Overview > Add Report** menu contains more high-level choices.

2. Click **Add Report** and select the report to add.



3. If necessary, move reports or delete other reports, as described in "What Can I Do From a Hosted Reporting Dashboard?" on page 28.

Apply a Filter to Report Data

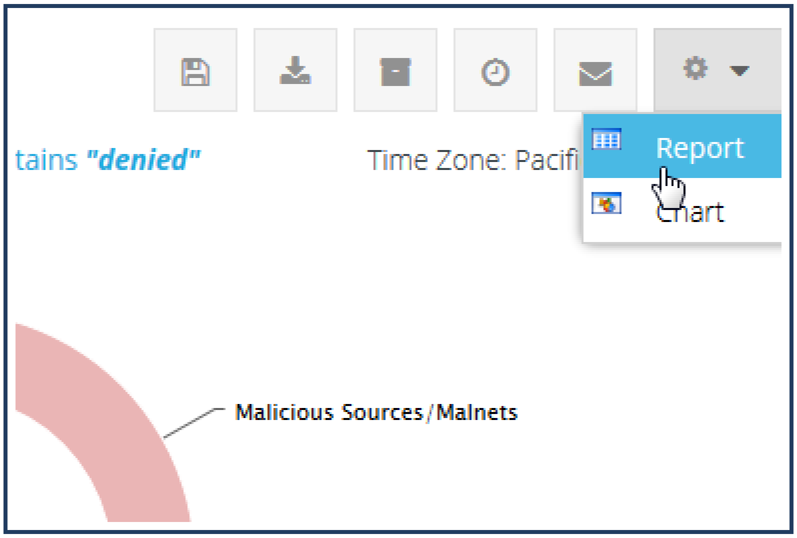
Most predefined Symantec Web Security Service reports display results that include a wide scope of data. When reviewing reports results, you can apply filters to limit the scope of the results.

Use Case

You run the **Blocked Requests by Category** report, which by default displays all categories that were blocked by policy (verdict = denied). You are curious to see the top ten users who were denied because they attempted to browse mature content websites.

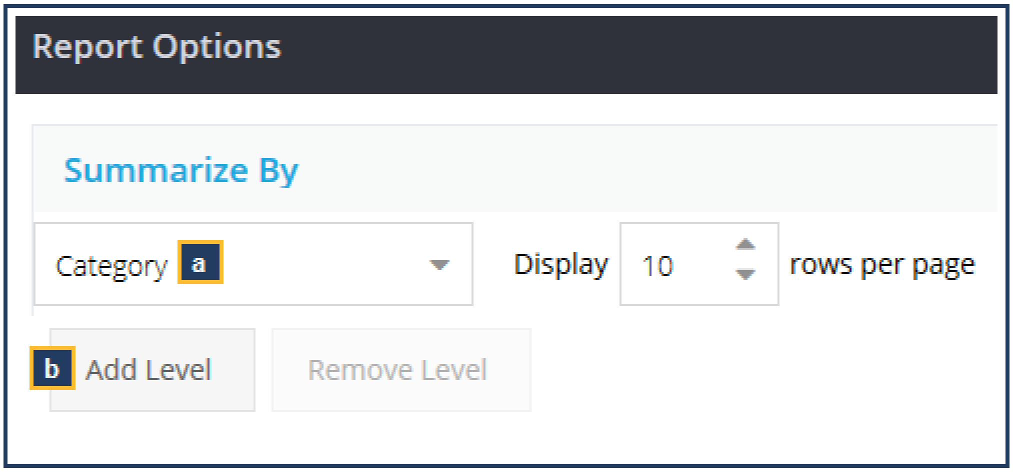
Procedure

1. From the reports, select **Options > Report**.



The service displays the Report Options dialog.

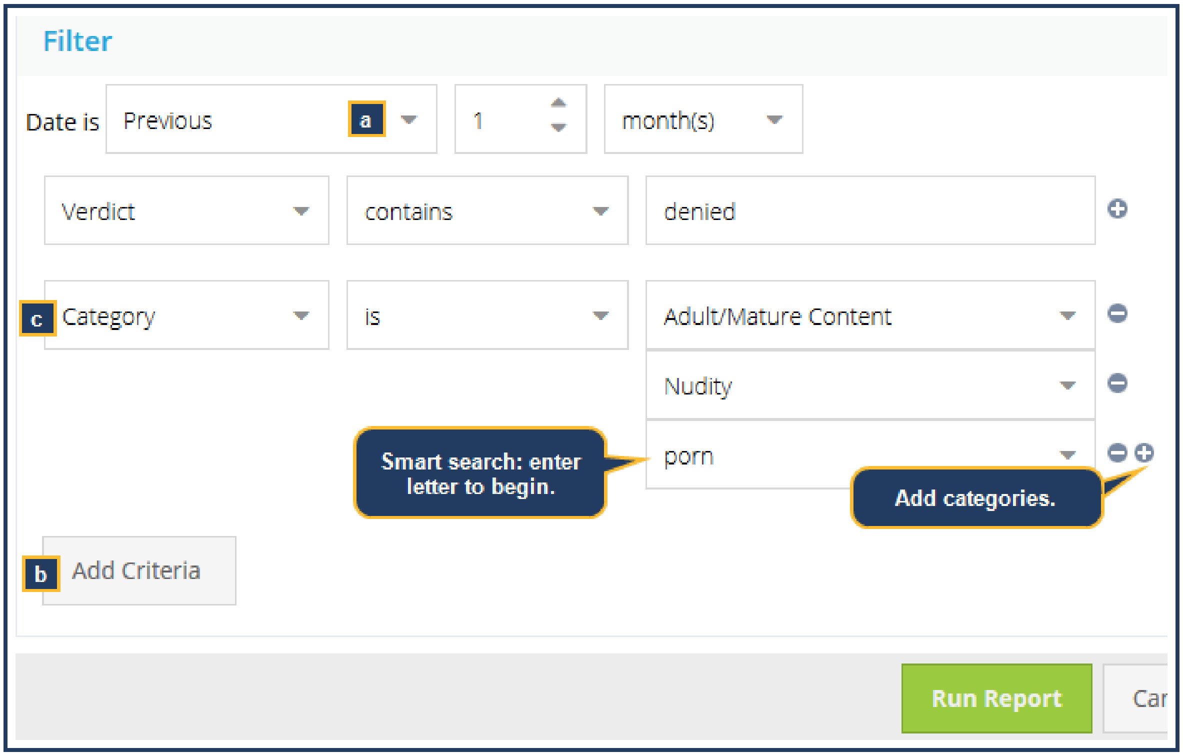
2. In the **Summarize By** area, determine by what criteria the report summarizes.



   a. For the above use case, keep **Category** as the primary summary datapoint. Define how many rows (per selection) per page display.

   b. (Optional) You can add one additional summary level by clicking **Add Level**. In this example, you want to see the top ten users per category.

3. In the **Filter** area, specify the date range and additional criteria.



Filter

Date is Previous | 1 | month(s)

Verdict | contains | denied

Category | is | Adult/Mature Content
Nudity
porn

Smart search: enter letter to begin.

Add categories.

   a. For the **Date is** criteria, specify what date range the report covers (if the Web Security Service did not process data for the specified date range, the report is blank).

   b. The filter automatically contains the default intent of the original report. In the above example, the **Blocked Requests per Category** report applies the **Verdict contains denied** (policy denied) filter. Click **Add Criteria**to add a new line. You can add multiple lines; the more you add, the more targeted the report becomes.

   c. Select the filter category. To continue with the example, select **Category**, **is**, and **Adult/Mature Content**. Click the **+** icon to add more **Category** filters. This examples searches for all denied verdicts because of four specific mature content categories.

4. Click **Save**. The filtered report generates and displays. If the filter did not result in useful data, select **Report > Options** again and adjust the filter.

5. Click links within the report, such as user names, to view even more detailed information.

6. To change the report graphic, select **Options > Chart**.

7. If the report is useful and you want to retain it or disseminate it, see "What Can I Do With Reports?" on page 32

Change the Graphic Within a Report

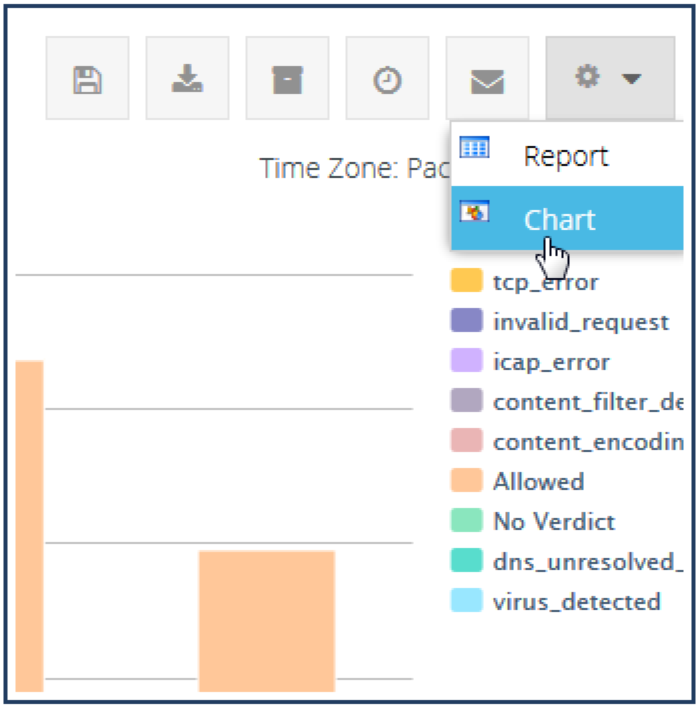
Each generated SymantecWeb Security Service report displays a graph that Symantec selected as the most effective for the data. You have the option to change not only the graphic, but the data that the Web Security Service uses to generate the graphic.

Use Case

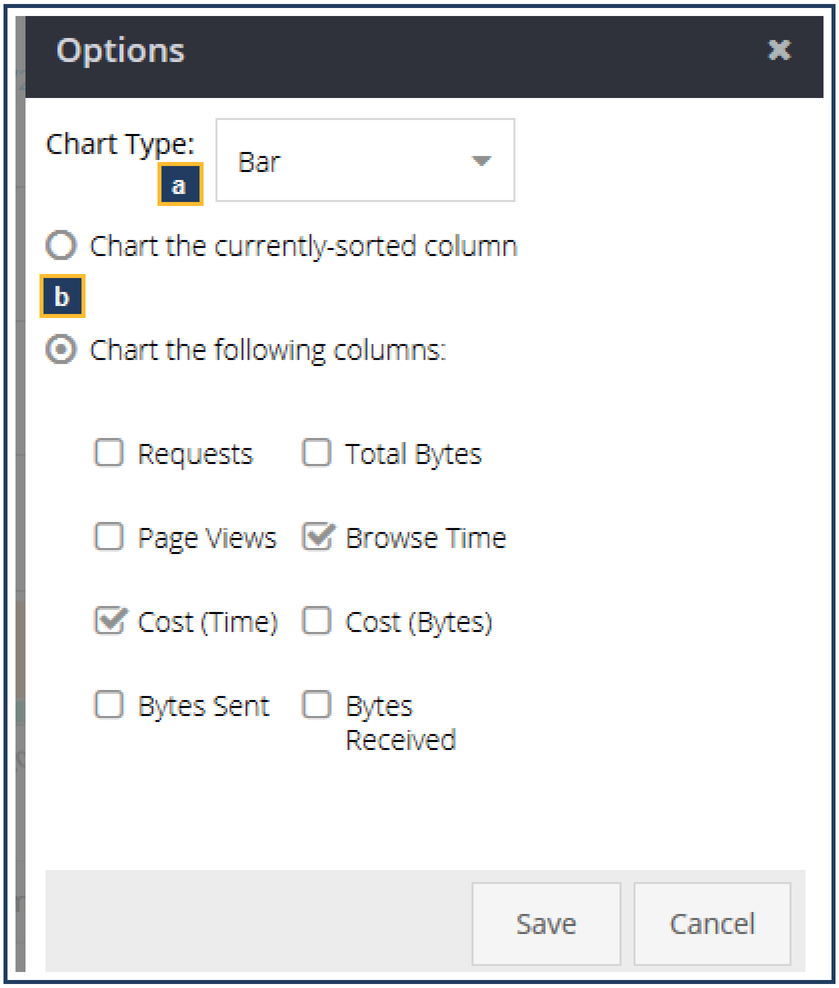
The **Search Engines > Reports > Web Applications** report by default generates a pie chart based on total requests for each application; however, you want to change the report to view the data in terms of costs.

Procedure

1. In Solutions mode, generate any report.
2. Next to the report name, select **Options > Chart** (gear icon). The portal displays the Options dialog.



3. In the Options dialog, select the components of the new graph.



Options

Chart Type: Bar

○ Chart the currently-sorted column

● Chart the following columns:

□ Requests □ Total Bytes

□ Page Views ☑ Browse Time

☑ Cost (Time) □ Cost (Bytes)

□ Bytes Sent □ Bytes Received

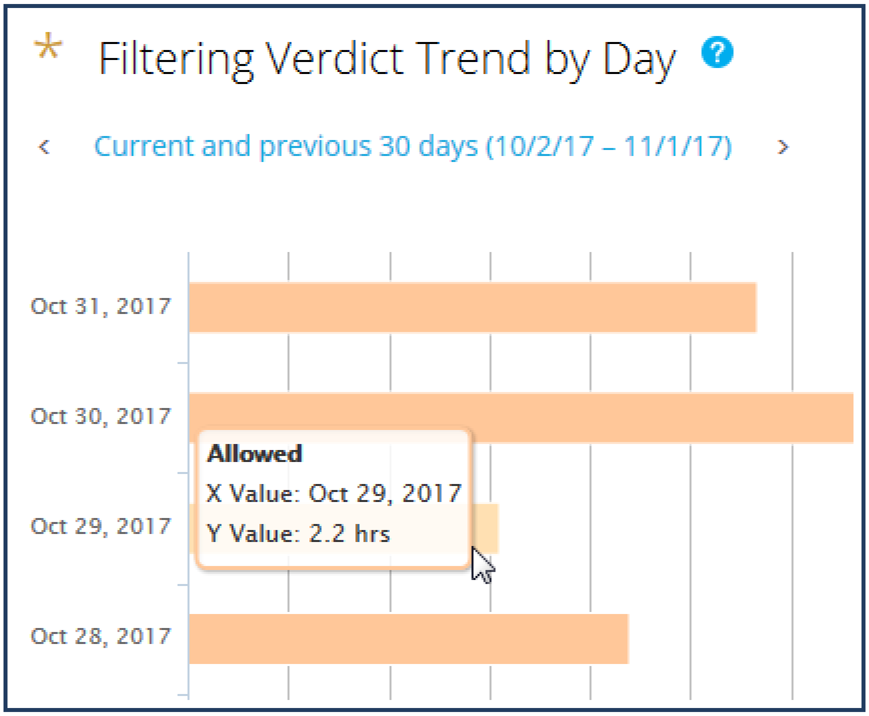
a. From the **Chart Type** drop-down, select a graph style.

b. The **Chart the currently-sorted column** option means the graphic compiles using the default data point. For example, a **...Per User** reports yields a graph based on user names but the report also contains other data columns. To change the graph source data, select **Chart the following column** and select an option or options.

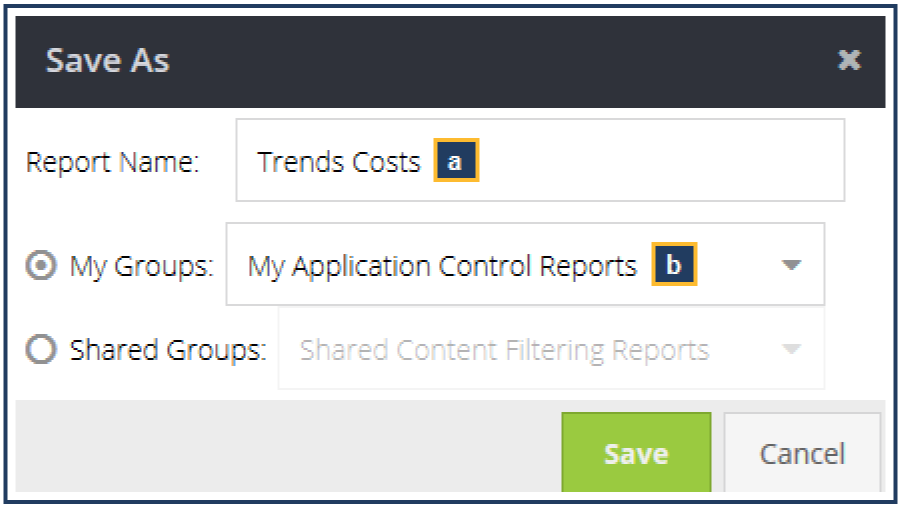
c. Click **Save**.

Some graph types, such as **Pie**, cannot contain more than one data element. The Web Security Service displays an error dialog if it cannot comply with your selections.

The service displays the new graph.



4.


Save As

Report Name: Trends Costs

● My Groups: My Application Control Reports

○ Shared Groups: Shared Content Filtering Reports

a. **Name** the new report.

b. Select which **Group** to save it in. If you save it in **My Groups**, only you can generate the report. If you save it in **Shared Groups**, anyone with access to this Web Security Service account sees the link and is able to run the report.

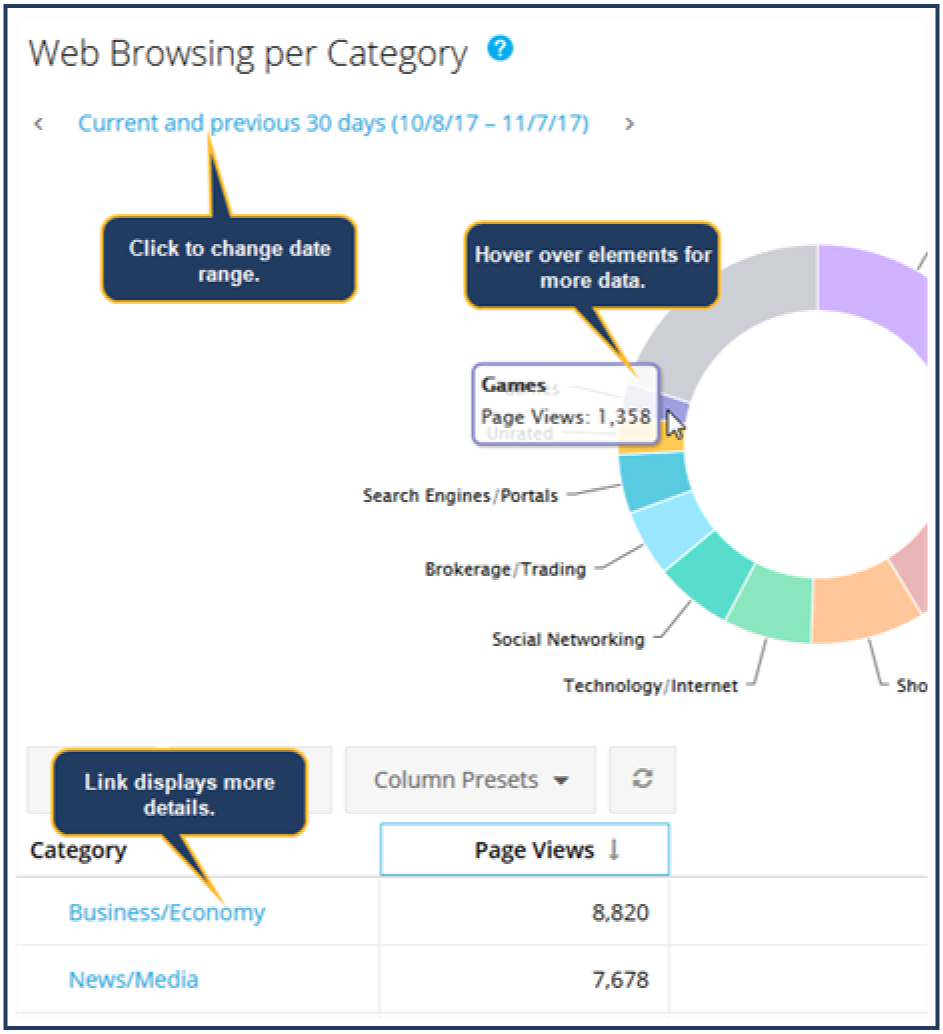
c. Click **Save**.

View Detailed Report Information

Every generated Symantec Web Security Service report contains dynamic elements that when accessed provide greater, more targeted data.

Links

Click any blue-colored link.



Web Browsing per Category

‹ Current and previous 30 days (10/8/17 – 11/7/17) ›

Click to change date range.

Hover over elements for more data.

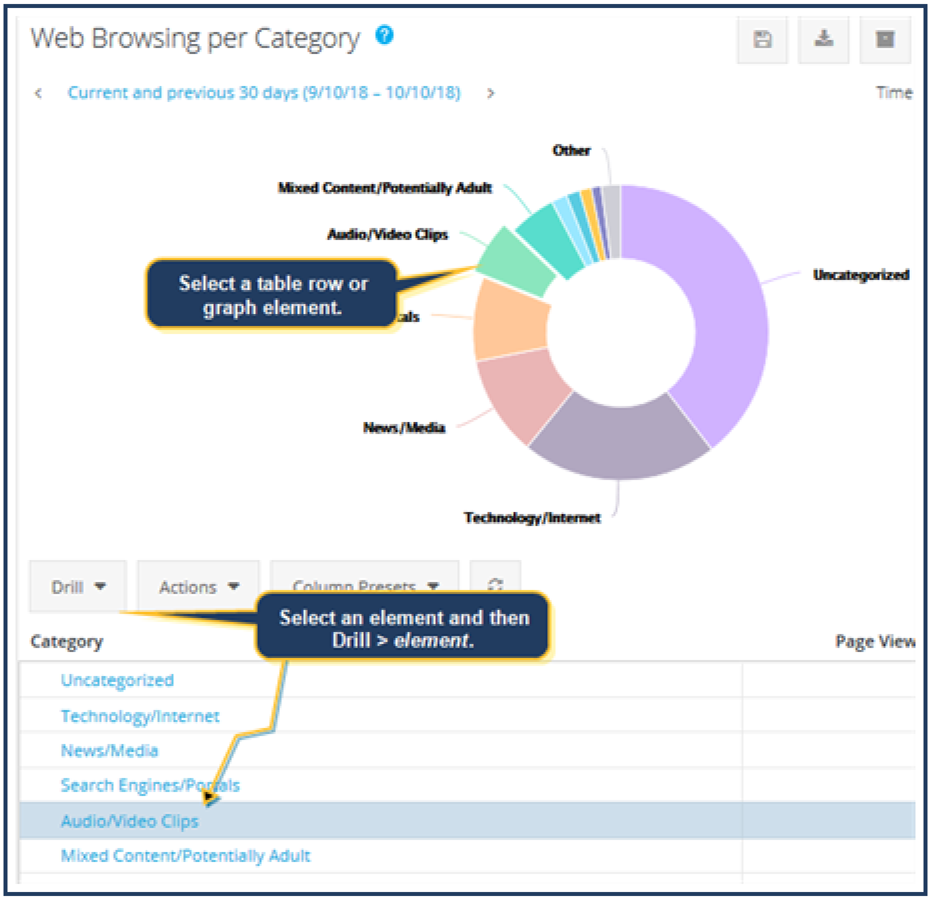
Games
Page Views: 1,358

Link displays more details.

Category	Page Views ↓
Business/Economy	8,820
News/Media	7,678

Drill Down to a Specific Element in a Report

1. Select a data row and click the **Drill** drop-down list.


Web Browsing per Category
Current and previous 30 days (9/10/18 - 10/10/18)
Time
Other
Mixed Content/Potentially Adult
Audio/Video Clips
Uncategorized
News/Media
Technology/Internet
Drill
Actions
Column Presets

Select a table row or graph element.

Select an element and then Drill > *element*.

Category	Page View
Uncategorized	
Technology/Internet	
News/Media	
Search Engines/Portals	
Audio/Video Clips	
Mixed Content/Potentially Adult	

2. Select an element to view (not all elements are available for all reports). For example, in the **Web Browsing per Category** report, you see there were several requests for **Shopping** category sites and you want to see which users requested them. Select **Drill > User**.

Required Log Fields

Before uploading access logs to the Web Security Service service from the staging sever, Symantec recommends running the **LogChecker** application (downloaded during the initial configuration and saved to the access log staging server) to verify that they are the correct format. This section provides the log field reference.

- Required Fields
  - `date`
  - `time`
  - `cs-host`
  - `cs(Referer)`
  - `sc-status`
  - `cs-uri-scheme`
- Recommended Fields
  - `c-ip`
  - `cs-username`
  - `x-exception-id`
  - `cs-categories`
  - `s-action`
  - `rs(Content-Type)`
  - `cs-uri-path`
  - `cs-uri-query`
  - `x-virus-id`