

Reporting and Alerting

This topic contains the following sections:

- Generate Reports to Monitor End-user Activity, on page 1
- Secure Appliance Reports, on page 12
- Secure Appliance Reports on the New Web Interface, on page 26

Generate Reports to Monitor End-user Activity

This topic contains the following sections:

- Overview of Reporting , on page 1
- Using the Reporting Pages, on page 3
- Using the Interactive Report Pages on the New Web Interface, on page 8
- Enabling Reporting, on page 8
- Scheduling Reports, on page 9
- Generating Reports On Demand, on page 11
- Archived Reports, on page 11
- Troubleshooting L4 Traffic Monitor Reports , on page 11

Overview of Reporting

The Secure Web Appliance generates high-level reports, allowing you to understand what is happening on the network and also allowing you to view traffic details for a particular domain, user, or category. You can run reports to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals.

Related Topics

- Printing and Exporting Reports from Report Pages, on page 6

Working with Usernames in Reports

When you enable authentication, reports list users by their usernames when they authenticate with the Web Proxy. By default, usernames are written as they appear in the authentication server. However, you can choose to make usernames unrecognizable in all reports.

Note Administrators always see usernames in reports.

Procedure

Step 1 Choose **Security Services > Reporting**, and click **Edit Settings**.

Step 2 Under Local Reporting, select **Anonymize usernames in reports**.

Step 3 Submit and Commit Changes.

Report Pages

The Secure Web Appliance offers the following reports:

- My Dashboard (the reporting "homepage"; can also be accessed by clicking the Home icon in the left edge of the menu bar)
- Overview
- Users
- User Count
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Advanced Malware Protection
- File Analysis
- AMP Verdict Updates
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- SOCKS Proxy
- Reports by User Location
- Web Tracking

- System Capacity
- System Status
- Scheduled Reports
- Archived Reports

Using the Reporting Pages

The various report pages provide an overview of system activity and support multiple options for viewing the system data. You can also search each page for Website and client-specific data.

You can perform the following tasks on most report pages:

Option	Link to Task
Change the time range displayed by a report	Changing the Time Range, on page 3
Search for specific clients and domains	Searching Data, on page 4
Choose which data to display in charts	Choosing Which Data to Chart , on page 5
Export reports to external files	Printing and Exporting Reports from Report Pages, on page 6

Changing the Time Range

You can update the data displayed for each security component using the Time Range field. This option allows you to generate updates for predefined time ranges and it allows you to define custom time ranges from a specific start time to a specific end time.



Note The time range you select is used throughout all of the report pages until you select a different value in the Time Range menu.

Time Range	Data is returned in...
Hour	Sixty complete minutes plus up to 5 additional minutes.
Day	One-hour intervals for the last 24 hours and including the current partial hour.
Week	On- day intervals for the last 7 days plus the current partial day.
Month (30 days)	One-day intervals for the last 30 days plus the current partial day.
Yesterday	The last 24 hours (00:00 to 23:59) using the time zone defined on the Secure Web Appliance.
Custom Range	The custom time range you defined. When you choose Custom Range, a dialog box appears to let you enter start and end times.

Note All reports display date and time information based on the system's configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT only to accommodate multiple systems in multiple time zones around the world.

Choosing a Time Range for Reports

Most predefined report pages allow you to choose a Time Range for the data to include. The time range that you select is used for all of the report pages until you select a different value in the Time Range menu.

Available Time Range options differ by appliance and differ for Email and Web reporting on the Security Management appliance:

Note Time ranges on report pages are displayed as a Greenwich Mean Time (GMT) offset. For example, Pacific time is GMT + 7 hours (GMT + 07:00).

Note All reports display date and time information based on the systems configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT to accommodate multiple systems in multiple time zones around the world.

Searching Data

Some reports include a field you can use to search for particular data points. When you search for data, the report refines the report data for the particular data set you are searching. You can search for values that exactly match of the string you enter, or for values that start with the string you enter. The following report pages include search fields:

Search Fields	Description
Users	Search for a user by user name or client IP address.
Web Sites	Search for a server by domain or server IP address.
URL Categories	Search for a URL category.
Application Visibility	Search for an application name that the AVC or ADC engine monitors and blocks.
Client Malware Risk	Search for a user by user name or client IP address.

Note You need to configure Authentication to view client user IDs as well as client IP addresses.

Choosing Which Data to Chart

The default charts on each Web Reporting page display commonly referenced data, but you can choose to chart different data instead. If a page has multiple charts, you can change each chart. The chart options are the same as the columns headings of the table(s) in the report.

Procedure

Step 1 Click the **Chart Options** link below a chart.

Step 2 Choose the data to display.

Step 3 Click **Done**.

Custom Reports

You can create a custom report page by assembling charts (graphs) and tables from existing report pages.

To	Do This
Add modules to your custom report page	See: • Modules That Cannot Be Added to Custom Reports , on page 5. • Creating Your Custom Report Page , on page 6
View your custom report page	1. Choose **Monitor > Email or Web > Reporting > Reporting > My Reports.** 2. Select the time range to viewThe time range selected applies to all reports, including all modules on the My Reports page. Newly-added modules appear at the top of the relevant section.
Rearrange modules on your custom report page	Drag and drop modules into the desired location.
Delete modules from your custom report page	Click the [X] in the top right corner of the module.
Generate a PDF or CSV version of your custom report	Choose **Reporting > Archived Reports** and click **Generate Report Now**.
Periodically generate a PDF or CSV version of your custom report	Choose **Reporting > Scheduled Reports.**

Modules That Cannot Be Added to Custom Reports

- Search results , including Web Tracking search results

Creating Your Custom Report Page

Before you begin

- Ensure that the modules that you want to add can be added. See Modules That Cannot Be Added to Custom Reports , on page 5.
- Delete any default modules that you do not need by clicking the [**X**] in the top right corner of those module.

Procedure

Step 1 Use one of the following methods to add a module to your custom report page:

Note
Some modules are available only using one of these methods. If you cannot add a module using one method, try another method.

- Navigate to the report page under the that has the module you want to add, then click the [+] button at the top of the module.
- Go to **Reporting** > **My Reports**, click the [+] button at the top of one of the sections, then select the report module that you want to add. You may need to click the [+] button in each section on the My Reports page in order to find the module that you are looking for.

  You can add each module only once; if you have already added a particular module to your report, the option to add it will not be available.

Step 2 If you add a module that you have customized (for example, by adding, deleting, or reordering columns, or by displaying non-default data in the chart), customize the modules on the My Reports page.

Modules are added with default settings. Time range of the original module is not maintained.

Step 3 If you add a chart that includes a separate legend (for example, a graph from the Overview page), add the legend separately. If necessary, drag and drop it into position beside the data it describes.

Subdomains vs. Second-level Domains in Reporting and Tracking

In reporting and tracking searches, second-level domains (regional domains listed at http://george.surbl.org/two-level-tlds) are treated differently from subdomains, although the two domain types may appear to be the same. For example:

- Reports will not include results for a two-level domain such as `co.uk` , but will include results for `foo.co.uk` . Reports include subdomains under the main corporate domain, such as `cisco.com` .
- Tracking search results for the regional domain `co.uk` will not include domains such as `foo.co.uk` , while search results for `cisco.com` will include subdomains such as `subdomain.cisco.com` .

Printing and Exporting Reports from Report Pages

You can generate a printer-formatted PDF version of any report page by clicking the **Printable (PDF)** link at the top-right corner of the page. You can also export raw data as a comma-separated value (CSV) file by clicking the **Export** link.

Because CSV exports include only raw data, exported data from a Web-based report page may not include calculated data such as percentages, even if that data appears in the Web-based report.

Exporting Report Data

Most reports include an **Export** link that allows you to export raw data to a comma-separated values (CSV) file. After exporting the data to a CSV file, you can access and manipulate the data in it using applications such as Microsoft Excel.

The exported CSV data displays all message tracking and reporting data in Greenwich Mean Time (GMT) regardless of the time zone set on the Secure Web Appliance. The purpose of the GMT time conversion is to allow data to be used independently from the appliance, or when referencing data from appliances in multiple time zones.

The following example is an entry from a raw data export of the Anti-Malware category report, where Pacific Daylight Time (PDT) is displayed as GMT 07:00 hours:

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
 Transactions Monitored, Transactions Blocked, Transactions Detected
 1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100,
2625
```

Category Header	Value	Description
`Begin Timestamp`	`1159772400.0`	Query start time in number of seconds from epoch.
`End Timestamp`	`1159858799.0`	Query end time in number of seconds from epoch.
`Begin Date`	`2006-10-02 07:00 GMT`	Date the query began.
`End Date`	`2006-10-03 06:59 GMT`	Date the query ended.
`Name`	`Adware`	Name of the malware category.
`Transactions Monitored`	`525`	Number of transactions monitored.
`Transactions Blocked`	`2100`	Number of transactions blocked.
`Transactions Detected`	`2625`	Total number of transactions = (Number of transactions detected) + (Number of transactions blocked).

Note - Category headers are different for each type of report.

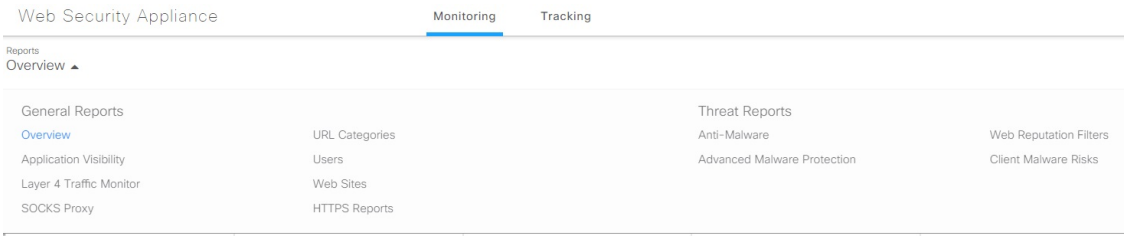
- If you export localized CSV data, the headings may not be rendered properly in some browsers. This occurs because some browsers may not use the proper character set for the localized text. To work around this problem, you can save the file to your local machine, and open the file in any Web browser using **File > Open**. When you open the file, select the character set to display the localized text.

Using the Interactive Report Pages on the New Web Interface

You can view the reports for the Secure Web Appliance using the **Reports** drop-down as shown in the following figure:

Note The Overview report page is the landing page (the page displayed after login). Reloading the new web interface from any reporting or tracking page loads the default landing page (Overview report page).

Figure 1: Reports Drop-down



The web reports as categorized as: **General Reports** and **Threat Reports**.

To access the new web interface, see Secure Appliance Reports on the New Web Interface.

Related Topics

- (Web Reports Only) Choosing Which Data to Chart, on page 49

Enabling Reporting

If your organization has multiple Secure Web Appliances and uses a Cisco Content Security Management Appliance to manage and view aggregated report data, you must enable centralized reporting on each Secure Web Appliance.

You can choose the type of reporting based on the appliance setup. You can choose to retain all reports locally. If your organization has multiple Secure Web Appliances and uses a Cisco Content Security Management Appliance, you can choose centralized reporting to manage and view aggregated report data. If you choose Centralized Reporting or local reporting , you have to apply these selections on each Secure Web Appliance.

Procedure

Step 1 Choose **Security Services** > **Reporting**, and click **Edit Settings**.

a) Select **Local Reporting** to enable reporting on the appliance. The reports will be accessible after logging in to the appliance portal.

b) Select **Centralized Reporting** to enable reporting through Cisco Content Security Management Appliance.

The Secure Web Appliance only stores all its collected data for local reporting. If Centralized Reporting is enabled on the appliance, then the Secure Web Appliance retains *only* System Capacity and System Status data, and those are the only reports available on the Secure Web Appliance locally.

See the topic "Using Centralized Web Reporting and Tracking" in your Cisco Content Security Management Appliance user guide for information about configuring this feature on the management appliance.

Step 2 **Submit** and Commit Changes.

Scheduling Reports

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, or previous month.

You can schedule reports for the following types of reports:

- Overview
- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Advanced Malware Protection
- Advanced Malware Protection Verdict Updates
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- SOCKS Proxy
- Reports by User Location
- System Capacity
- My Dashboard

Adding a Scheduled Report

Procedure

Step 1 Choose **Reporting** > **Scheduled Reports** and click **Add Scheduled Report**.

Step 2 Choose a report **Type**.

Step 3 Enter a descriptive **Title** for the report.

Avoid creating multiple reports with the same name.

Step 4 Choose a time range for the data included in the report.

Step 5 Select the **Format** for the generated report.

The default format is PDF. Most reports also allow you to save raw data as a CSV file.

Step 6 Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.

Step 7 In the **Schedule** section, choose whether to run the report daily, weekly, or monthly, and at what time.

Step 8 In the **Email to** field, enter the email address(es) to which the generated report is to be sent.

If you do not specify an email address, the report is simply archived.

Step 9 Choose a **Report Language** for the data.

Step 10 Submit and Commit Changes.

Editing Scheduled Reports

Procedure

Step 1 Choose **Reporting > Scheduled Reports**.

Step 2 Select the report title from the list.

Step 3 Modify settings.

Step 4 Submit and Commit Changes.

Deleting Scheduled Reports

Procedure

Step 1 Choose **Reporting > Scheduled Reports**.

Step 2 Select the check boxes corresponding to the reports that you want to delete.

Step 3 To remove all scheduled reports, select the **All** check box.

Step 4 **Delete** and **Commit** Changes.

Note
Archived versions of deleted reports are not deleted.

Generating Reports On Demand

Procedure

Step 1 Choose **Reporting > Archived Reports**.

Step 2 Click **Generate Report Now.**

Step 3 Choose a report **Type**.

Step 4 Enter a descriptive **Title** for the report.

Avoid creating multiple reports with the same name.

Step 5 Choose a time range for the data included in the report.

Step 6 Select the **Format** for the generated report.

The default format is PDF. Most reports also allow you to save raw data as a CSV file.

Step 7 Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.

Step 8 Select one of the **Delivery Options**:

- **Archive** the report (the report will appear on the Archived Reports page).
- **Email now to recipients**; provide one or more email addresses.

Step 9 Choose a **Report Language** for the data.

Step 10 Click **Deliver this Report** to generate the report.

Step 11 Commit Changes.

Archived Reports

The **Reporting > Archived Reports** page lists available archived reports. Each name in the Report Title column provides a link to a view of that report. The **Show** menu filters the types of reports that are listed. The column headings can be clicked to sort the data in each column.

The appliance stores up to 12 instances of each scheduled report (up to a total of 1000 reports). Archived reports are stored in the `/periodic_reports` directory on the appliance. Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 12 instances applies to each scheduled report with the same name and time range.

Troubleshooting L4 Traffic Monitor Reports

If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy's data port is recorded and displayed as the client IP address in reports. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses. To do this, see the IronPort AsyncOS for Web User Guide.

Related Topics

- Client Malware Risk Page, on page 18
- Searching for Transactions Processed by the L4 Traffic Monitor , on page 24

Secure Appliance Reports

This topic contains the following sections:

- Overview Page, on page 12
- Users Page, on page 14
- User Count Page, on page 15
- Web Sites Page, on page 15
- URL Categories Page, on page 16
- Application Visibility Page, on page 16
- Anti-Malware Page, on page 17
- Advanced Malware Protection Page, on page 18
- File Analysis Page, on page 18
- AMP Verdict Updates Page , on page 18
- Client Malware Risk Page, on page 18
- Web Reputation Filters Page, on page 19
- L4 Traffic Monitor Page, on page 19
- SOCKS Proxy Page , on page 20
- Reports by User Location Page, on page 20
- Web Tracking Page , on page 21
- System Capacity Page, on page 24
- System Status Page, on page 25

Overview Page

The **Reporting > Overview** page provides a synopsis of the activity on the Secure Web Appliance. It includes graphs and summary tables for Web traffic processed by the Secure Web Appliance.

Table 1: System Overview

Section	Description
Web Proxy Traffic Characteristics	`Listing of Average transactions per second in past minute`, `Average bandwidth (bps) in past minute`, `Average response time (ms) in past minute`, and `Total current connections`.

Section	Description
System Resource Utilization	Listing of current `Overall CPU Load`, `RAM` and `Reporting / logging disk` usage. Click **System Status Details** to switch to the System Status page (see System Status Page on the New Web Interface, on page 59 for details). **Note** The CPU utilization value shown on this page and the CPU value shown on the System Status page may differ slightly because they are read separately, at differing moments.

Table 2: Time Range-based Categories and Summaries

Section	Description
Time Range: Choose a time range for the data displayed in the following sections. Options are Hour, Day, Week, 30 Days, Yesterday, or a Custom Range.	
Total Web Proxy Activity	Displays the actual number of transactions (vertical scale) as well as the approximate date that the (Web Proxy) activity occurred (horizontal timeline).
Web Proxy Summary	Allows you to view the percentage of Web Proxy activity that are suspect or clean Web Proxy activity.
L4 Traffic Monitor Summary	Reports on traffic monitored and blocked by the L4 Traffic Monitor.
Suspect Transactions	Allows you to view the web transactions that have been labeled as suspect by the various security components. Displays the actual number of transactions as well as the approximate date that the activity occurred.
Suspect Transactions Summary	Allows you to view the percentage of blocked or warned transactions that are suspect.
Top URL Categories: Total Transactions	Displays the top 10 URL categories that have been blocked.
Top Application Types: Total Transactions	Displays the top application types that have been blocked by the AVC or ADC engine.
Top Malware Categories: Monitored or Blocked	Displays all malware categories that have been detected.
Top Users: Blocked or Warned Transactions	Displays the users that are generating the blocked or warned transactions. Authenticated users are displayed username and unauthenticated users are displayed by IP address.
Web Traffic Tap Status	Displays the untapped and tapped traffic transactions in a graph format.
Web Traffic Tap Summary	Displays the summary of the tapped and untapped traffic transactions along with the total traffic transactions.
Tapped HTTP/HTTPS Traffic	Displays the tapped HTTP and HTTPS traffic transactions in a graph format.
Tapped Traffic Summary	Displays the summary of HTTP and HTTPS traffic transactions along with the total HTTP/HTTPS traffic transactions.

Section	Description
EUP Transactions	Displays encapsulated URL transactions. These are transactions that were performed through websites like *translate.google.com*.
EUP Transaction Summary	Displays the summary of encapsulated URL transactions.
EUP Suspect Transactions	Displays the encapsulated URL transactions that were found to be suspect.
EUP Suspect Transaction Summary	Displays the summary of encapsulated URL transactions that were found to be suspect.

Users Page

The **Reporting > Users** page provides several links that allows you to view web traffic information for individual users. You can view how much time users on the network have spent on the Internet or on a particular website or URL, and how much bandwidth users have used.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Users by Transactions Blocked	Lists the users (vertical scale) that have the greatest number of blocked transactions (horizontal scale).
Top Users by Bandwidth Used	Displays the users (vertical scale) that are using the most bandwidth on the system (horizontal scale represented in gigabyte usage).
Users Table	Lists individual users and displays multiple statistics on each user.

User Details Page

The **User Details** page displays information about a specific user selected in the Users Table on the **Reporting > Users** page.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
URL Categories by Total Transactions	Lists the specific URL categories that a specific user is using.
Trend by Total Transaction	Displays at what times the user accessed the web.
URL Categories Matched	Shows all matched URL categories during a specified time range for both completed and blocked transactions.

Section	Description
Domains Matched	Displays information about a specific Domain or IP address that this user has accessed. **Note** If you export this Domains data to a CSV file, be aware that only the first 300,000 entries are exported to the file.
Applications Matched	Displays specific application that a specific user is using as detected by the AVC or ADC engine.
Malware Threats Detected	Displays the top malware threats that a specific user is triggering.
Policies Matched	Displays a specific policy that is being enforced on this particular user.

User Count Page

The **Reporting** > **User Count** page displays information about the total number of authenticated and unauthenticated users of the appliance. The page lists the unique user count for the last 30 days, 90 days, and 180 days.



Note System computes the total user count of authenticted and unauthenticated users once a day.

For example, if you view the user count report on May 22, 23:59, at the latest, the system will display the total user count till May 22, 00:00.

Web Sites Page

The **Reporting > Web Sites** page is an overall aggregation of the activity that is happening on the Secure Web Appliance.

Section	Description
Time Range (drop-down list)	Menu allows you to choose the time range of the data contained in the report.
Top Domains by Total Transactions	Lists the top domains that are being visited on the site in a graph format.
Top Domains by Transactions Blocked	Lists the top domains that triggered a block action to occur per transaction in a graph format.
Domains Matched	Lists the domains that are that are being visited on the site in an interactive table. **Note** If you export this Domains data to a CSV file, be aware that only the first 300,000 entries are exported to the file.

URL Categories Page

The **Reporting > URL Categories** page can be used to view the URL categories that are being visited by users on the network. The URL Categories page can be used in conjunction with the Application Visibility Page and the Users Page to investigate a particular user and also what types of applications or websites that a particular user is trying to access.



Note The set of predefined URL categories is occasionally updated.

Section	Description
Time Range (drop-down list)	Choose the time range for your report.
Top URL Categories by Total Transactions	This section lists the top URL categories that are being visited on the site in a graph format.
Top URL Categories by Blocked and Warned Transactions	Lists the top URL that triggered a block or warning action to occur per transaction in a graph format.
URL Categories Matched	Shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category. If the percentage of uncategorized URLs is higher than 15-20%, consider the following options: • For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. • You can report uncategorized and misclassified and URLs to the Cisco for evaluation and database update. • Verify that Web Reputation Filtering and Anti-Malware Filtering are enabled.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated automatically on your Secure Web Appliance.

When these updates occur, old category names will continue to appear in reports until the data associated with the older categories is too old to be included in reports. Report data generated after a URL category set update will use the new categories, so you may see both old and new categories in the same report.

Application Visibility Page

The **Reporting > Application Visibility** page shows the applications and application types used and blocked as detected by the Application Visibility and Control or Application Discovery and Control engine.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Application Types by Total Transactions	This section lists the top application types that are being visited on the site in a graph format.
Top Applications by Blocked Transactions	Lists the top application types that triggered a block action to occur per transaction in a graph format.
Application Types Matched	Allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions graph.
Applications Matched	Shows all the application during a specified time range.

Anti-Malware Page

The **Reporting > Anti-Malware** page allows you to monitor and identify malware detected by the Cisco DVS engine.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Malware Categories Detected	Displays the top malware categories detected by the DVS engine.
Top Malware Threats Detected	Displays the top malware threats detected by the DVS engine.
Malware Categories	Displays information about particular malware categories that are shown in the Top Malware Categories Detected section.
Malware Threats	Displays information about particular malware threats that are shown in the Top Malware Threats section.

Malware Category Report Page

Procedure

Step 1 Choose **Reporting > Anti-Malware**.

Step 2 In the Malware Categories interactive table, click on a category in the Malware Category column.

Malware Threat Report Page

Procedure

Step 1 Choose **Reporting** > **Anti-Malware**.

Step 2 In the Malware Threat table, click on a category in the Malware Category column.

Advanced Malware Protection Page

See File Reputation Filtering and File Analysis.

File Analysis Page

See File Reputation and File Analysis Reporting and Tracking.

AMP Verdict Updates Page

See File Reputation Filtering and File Analysis.

Client Malware Risk Page

The **Reporting** > **Client Malware Risk** page is a security-related reporting page that can be used to monitor client malware risk activity. The Client Malware Risk page also lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM).

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report.
Web Proxy: Top Clients by Malware Risk	This chart displays the top ten users that have encountered a malware risk.
L4 Traffic Monitor: Malware Connections Detected	This chart displays the IP addresses of the computers in your organization that most frequently connect to malware sites.
Web Proxy: Clients by Malware Risk	The Web Proxy: Clients by Malware Risk table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section.
L4 Traffic Monitor: Clients by Malware Risk	This table displays IP addresses of computers in your organization that frequently connect to malware sites.

Client Detail Page for Web Proxy - Clients by Malware Risk

The **Client Details** page shows all the web activity and malware risk data for a particular client during the specified time range.

Procedure

Step 1 Choose **Reporting > Client Malware Risk**.

Step 2 In the **Web Proxy - Client Malware Risk** section, click a user name in the "User ID / Client IP Address" column.

What to do next

User Details Page, on page 14

Web Reputation Filters Page

The **Reporting > Web Reputation Filters** page is a security-related reporting page that allows you to view the results of your set Web Reputation Filters for transactions during a specified time range.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Web Reputation Actions (Trend)	Displays the total number of web reputation actions (vertical) against the time specified (horizontal timeline).
Web Reputation Actions (Volume)	Displays the web reputation action volume in percentages by transactions.
Web Reputation Threat Types by Blocked Transactions	Displays the threat types that were blocked due to a low reputation score.
Web Reputation Threat Types by Scanned Further Transactions	Displays the threat types that resulted in a reputation score that indicated to scan the transaction.
Web Reputation Actions (Breakdown by Score)	Displays the web reputation scores broken down for each action.

L4 Traffic Monitor Page

The **Reporting > L4 Traffic Monitor** page is a security-related reporting page that displays information about malware ports and malware sites that the L4 Traffic Monitor has detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

The L4 Traffic Monitor listens to network traffic that comes in over all ports on the appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

Section	Description
Time Range (drop-down list)	A menu that allows you to choose a time range on which to report.

Section	Description
Top Client IPs	Displays, in graph format, the IP addresses of computers in your organization that most frequently connect to malware sites.
Top Malware Sites	Displays, in graph format, the top malware domains detected by the L4 Traffic Monitor.
Client Source IPs	Displays the IP addresses of computers in your organization that frequently connect to malware sites.
Malware Ports	Displays the ports on which the L4 Traffic Monitor has most frequently detected malware.
Malware Sites Detected	Displays the domains on which the L4 Traffic Monitor most frequently detects malware.

SOCKS Proxy Page

The **Reporting > SOCKS Proxy** Page allows you to view data and trends for transactions processed through the SOCKS proxy, including information about top destinations and users.

Reports by User Location Page

The **Reporting > Reports by User Location** page allows you to find out what activities your local and remote users are conducting.

Activities include:

- URL categories that are being accessed by the local and remote users.
- Anti-Malware activity that is being triggered by sites the local and remote users are accessing.
- Web Reputation of the sites being accessed by the local and remote users.
- Applications that are being accessed by the local and remote users.
- Users (local and remote).
- Domains accessed by local and remote users.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Total Web Proxy Activity: Remote Users	Displays the activity of your remote users (vertical) over the specified time (horizontal).
Web Proxy Summary	Displays a summary of the activities of the local and remote users on the network.
Total Web Proxy Activity: Local Users	Displays the activity of your remote users (vertical) over the specified time (horizontal).

Section	Description
Suspect Transactions Detected: Remote Users	Displays the suspect transactions that have been detected due to Access Policies defined for remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	Displays a summary of suspected transactions of the remote users on the network.
Suspect Transactions Detected: Local Users	Displays the suspect transactions that have been detected due to Access Policies defined for your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	Displays a summary of suspected transactions of the local users on the network.

Web Tracking Page

Use the Web Tracking page to search for and get details about individual transactions or patterns of transactions that may be of concern. Depending on your needs, search in one of the following tabs:

Web Tracking Page	Link to Task
Transactions processed by the Web Proxy	Searching for Transactions Processed by the Web Proxy , on page 21
Transactions processed by the L4 Traffic Monitor	Searching for Transactions Processed by the L4 Traffic Monitor , on page 24
Transactions processed by the SOCKS Proxy	Searching for Transactions Processed by the SOCKS Proxy , on page 24

Alternatively, use FQDN to search for website data in the **Web Tracking** page for some cases like Transparent Passthrough.

Note A transparent request displays the name of the domain or server on the tracking page. However, when transparent requests, including transparent passthrough, are sent without SNI, the IP address is displayed.

Searching for Transactions Processed by the Web Proxy

You can use the **Proxy Services** tab on the **Reporting** > **Web Tracking** page to track and report on web usage for a particular user or for all users.

You can view search results for the type of transactions logged (blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.

Note The Web Proxy only reports on transactions that include an ACL decision tag other than OTHER-NONE.

Procedure

Step 1 Choose **Reporting** > **Web Tracking**.

Step 2 Click the **Proxy Services** tab.

Step 3 Configure the settings.

Setting	Description
Time Range	Choose the time range on which to report.
User/Client IP	(Optional) Enter an authentication username as it appears in reports or a client IP address that you want to track. You can also enter an IP range in CIDR format. When you leave this field empty, the search returns results for all users.
Website	(Optional) Enter a website that you want to track. When you leave this field empty, the search returns results for all websites. **Note** You can search for SNI (Server Name Indication). SNI, an extension of the TLS protocol, enables clients to securely specify hostnames while performing web transactions. You must specify entire words. For SNI to work, AMP, and Reputation Services must be enabled.
Transaction Type	Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.

Step 4 (Optional) Expand the Advanced section and configure the fields to filter the web tracking results with more advanced criteria.

Setting	Description
URL Category	To filter by a URL category, select **Filter by URL Category** and type the first letter of a URL category by which to filter. Choose the category from the list that appears.
Application	To filter by an application, select **Filter by Application** and choose an application by which to filter. To filter by an application type, select **Filter by Application Type** and choose an application type by which to filter.
Policy	To filter by the name of the policy responsible for the final decision on this transaction, select **Filter by Action Policy** and enter a policy group name (Access Policy, Decryption Policy, or Data Security Policy) by which to filter. See the description for PolicyGroupName in the section Web Proxy Information in Access Log Files for more information.
Advanced Malware Protection	See About Web Tracking and Advanced Malware Protection Features.

Setting	Description
Malware Threat	To filter by a particular malware threat, select **Filter by Malware Threat** and enter a malware threat name by which to filter. To filter by a malware category, select **Filter by Malware Category** and choose a malware category by which to filter.
WBRS	In the WBRS section, you can filter by web reputation score and by a particular web reputation threat. • To filter by web reputation score, select **Score Range** and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting **No Score**. • To filter by web reputation threat, select **Filter by Reputation Threat** and enter a web reputation threat by which to filter.
AnyConnect Secure Mobility	To filter by the location of users (either remote or local), select **Filter by User Location** and choose a user type by which to filter.
User Request	To filter by transactions that were initiated by the client, select **Filter by User-Requested Transactions**. **Note** When you enable this filter, the search results include some “best guess” transactions.
Encapsulated URL Protection	Enable this filter for encapsulated URL transactions. **Note** • You must enable the HTTPS Proxy. See Enabling the HTTPS Proxy • Ensure that the web reputation score range for https://translate.google.com is set to decrypt. See Configuring Web Reputation Filter Settings for Decryption Policy Groups

Step 5 Click **Search**.

Results are sorted by time stamp, with the most recent result at the top.

The number in parentheses below the “Display Details” link is the number of related transactions spawned by the user-initiated transaction, such as images loaded, javascripts run, and secondary sites accessed.

Step 6 (Optional) Click **Display Details** in the Transactions column to view more detailed information about each transaction.

Note
If you need to view more than 1000 results, click the **Printable Download** link to obtain a CSV file that includes the complete set of raw data, excluding details of related transactions.

Tip
If a URL in the results is truncated, you can find the full URL in the access log.

To view details for up to 500 related transactions, click the **Related Transactions** link.

What to do next

- URL Category Set Updates and Reports , on page 16
- Malware Category Descriptions
- About Web Tracking and Advanced Malware Protection Features

Searching for Transactions Processed by the L4 Traffic Monitor

The L4 Traffic Monitor tab on the **Reporting > Web Tracking** page provides details about connections to malware sites and ports. You can search for connections to malware sites by the following types of information:

- Time range
- Site, using IP address or domain
- Port
- IP address associated with a computer in your organization
- Connection type

The first 1000 matching search results are displayed.

Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; users; and destination domain, IP address, or port.

Procedure

Step 1 Choose **Web > Reporting > Web Tracking**.
Step 2 Click the **SOCKS Proxy** tab.
Step 3 To filter results, click **Advanced**.
Step 4 Enter search criteria.
Step 5 Click **Search**.

What to do next

SOCKS Proxy Page , on page 20

System Capacity Page

The **Reporting > System Capacity** page displays current and historical information about resource usage on the Secure Web Appliance.

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

- **Hour Report.** The Hour report queries the minute table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an minute by minute basis over a 60 minute period.
- **Day Report.** The Day report queries the hour table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table.

The Week Report and 30 Days Report work similarly to the Hour and Day Reports.

System Status Page

Use the **Reporting > System Status** page to monitor the System Status. This page displays the current status and configuration of the Secure Web Appliance.

This Section...	Displays
Secure Web Appliance Status	• System uptime • System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging. The CPU utilization value shown on this page and the CPU value shown on the system Overview page (Overview Page, on page 12) may differ slightly because they are read separately, at differing moments. RAM usage for a system that is working efficiently may be above 90%, because RAM that is not otherwise in use by the system is used by the web object cache. If your system is not experiencing serious performance issues and this value is not stuck at 100%, the system is operating normally. **Note** Proxy Buffer Memory is one component that uses this RAM.
Proxy Traffic Characteristics	• Transactions per second • Bandwidth • Response time • Cache hit rate • Connections
Web Traffic Tap	Web Traffic Tap CPU Utilization.
High Availability	Status of High Availability service.
External Services	• Identity Services Engine

This Section...	Displays
Current Configuration	Web Proxy settings: • Web Proxy Status — enabled or disabled. • Deployment Topology. • Web Proxy Mode — forward or transparent. • IP Spoofing — enabled or disabled. L4 Traffic Monitor settings: • L4 Traffic Monitor Status — enabled or disabled. • L4 Traffic Monitor Wiring. • L4 Traffic Monitor Action — monitor or block. Web Traffic Tap settings: • Web Traffic Tap Status — enabled or disabled • Web Traffic Tap Interface — P1, P2, TI, or T2 Secure Web Appliance Version Information Hardware information

Related Topics

System Capacity Page, on page 24

Secure Appliance Reports on the New Web Interface

This topic contains the following sections:

- Understanding the Web Reporting Pages on the New Web Interface, on page 26
- (Web Reports Only) Choosing Which Data to Chart, on page 49
- Web Tracking on the New Web Interface, on page 50
- Working with Web Tracking Search Results , on page 55
- Scheduling and Archiving Web Reports on the New Web Interface, on page 56
- System Status Page on the New Web Interface, on page 59

Understanding the Web Reporting Pages on the New Web Interface

The following table lists the reports under the Reports drop-down. available in the latest supported release of AsyncOS for Secure Web Appliances under the **Reports** drop-down of the web interface. For more information,

see Using the Interactive Report Pages on the New Web Interface, on page 8. If your Secure Web Appliances are running earlier releases of AsyncOS, not all of these reports are available.

Table 3: Web Reports Drop-down Options

Reports Drop-down Option	Action
General Reports	
Overview Page	The Overview page provides a synopsis of the activity on your Secure Web Appliances. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the Overview Page, on page 29.
Application Visibility Page	The Application Visibility page allows you to apply and view the controls that have been applied to a particular application types within the Security Management appliance and Secure Web Appliance. For more information, see the Application Visibility Page, on page 31.
Layer 4 Traffic Monitor Page	Allows you to view information about malware ports and malware sites that the L4 Traffic Monitor detected during the specified time range. For more information, see the Layer 4 Traffic Monitor Page, on page 32.
SOCKS Proxy Page	Allows you to view data for SOCKS proxy transactions, including destinations and users. For more information, see the SOCKS Proxy Page, on page 34.
URL Categories Page	The URL Categories page allows you to view the top URL Categories that are being visited, including: • The top URLs that have triggered a block or warning action to occur per transaction. • All the URL categories during a specified time range for both completed, warned and blocked transactions. This is an interactive table with interactive column headings that you can use to sort data as you need. For more information, see the URL Categories Page, on page 35.

Reports Drop-down Option	Action
Users Page	The Users page provides several web tracking links that allow you to view web tracking information for individual users. From the Users page you can view how long a user, or users, on your system have spent on the internet, on a particular site or URL, and how much bandwidth that user is using. From the Users page you can click on an individual user in the interactive Users table to view more details for that specific user on the User Details page. The User Details page allows you to see specific information about a user that you have identified in the Users table on the Users page. From this page you can investigate individual user's activity on your system. This page is particularly useful if you are running user-level investigations and need to find out, for example, what sites your users are visiting, what Malware threats they are encountering, what URL categories they are accessing, and how much time a specific user is spending at these sites. For more information, see the Users Page, on page 38. For information on a specific user in your system, see the User Details Page (Web Reporting) , on page 40.
Web Sites Page	The Web Sites page allows you to view an overall aggregation of the activity that is happening on your managed appliances. From this page you can monitor high-risk web sites accessed during a specific time range. For more information, see the Web Sites Page, on page 42.
HTTPS Reports	The HTTPS Reports report page is an overall aggregation of the HTTP/HTTPS traffic summary (transactions or bandwidth usage) on the managed appliances. For more information, see the HTTPS Reports Page, on page 37
Threat Reports	
Anti-Malware Page	The Anti-Malware page allows you to view information about malware ports and malware sites that the anti-malware scanning engine(s) detected during the specified time range. The upper part of the report displays the number of connections for each of the top malware ports and web sites. The lower part of the report displays malware ports and sites detected. For more information, see the Anti-Malware Page, on page 44.

Reports Drop-down Option	Action
Advanced Malware Protection Page	Advanced Malware Protection protects against zero-day and targeted file-based threats by obtaining the reputation of known files, analyzing behavior of certain files that are not yet known to the reputation service, and continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network. For more information, see Advanced Malware Protection Page, on page 42.
Client Malware Risk Page	The Client Malware Risk page is a security-related reporting page that can be used to identify individual client computers that may be connecting unusually frequently to malware sites. For more information, see the Client Malware Risks Page, on page 47.
Web Reputation Filters Page	Allows you to view reporting on Web Reputation filtering for transactions during a specified time range. For more information, see the Web Reputation Filters Page, on page 47.

About Time Spent

The Time Spent column in various tables represents the amount of time a user spent on a web page. For purposes of investigating a user, the time spent by the user on each URL category. When tracking a URL, the time spent by each user on that specific URL.

Once a transaction event is tagged as ‘viewed’, that is, a user goes to a particular URL, a ‘Time Spent’ value will start to be calculated and added as a field in the web reporting table.

To calculate the time spent, AsyncOS assigns each active user with 60 seconds of time for activity during a minute. At the end of the minute, the time spent by each user is evenly distributed among the different domains the user visited. For example, if a user goes to four different domains in an active minute, the user is considered to have spent 15 seconds at each domain.

For the purposes of the time spent value, considering the following notes:

- An active user is defined as a user name or IP address that sends HTTP traffic through the appliance and has gone to a website that AsyncOS considers to be a “page view.”
- AsyncOS defines a page view as an HTTP request initiated by the user, as opposed to a request initiated by the client application. AsyncOS uses a heuristic algorithm to make a best effort guess to identify user page views.

Units are displayed in Hours:Minutes format.

Overview Page

The **Overview** report page provides a synopsis of the activity on your Secure Web Appliances. It includes graphs and summary tables for the incoming and outgoing transactions.

To view the Overview report page, choose **Monitoring > Overview** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

At a high level the **Overview** report page shows you statistics about the URL and User usage, Web Proxy activity, and various transaction summaries. The transaction summaries gives you further trending details on, for example suspect transactions, and right across from this graph, how many of those suspect transactions are blocked and in what manner they are being blocked.

The lower half of the Overview report page is about usage. That is, the top URL categories being viewed, the top application types and categories that are being blocked, and the top users that are generating these blocks or warnings.

Table 4: Details on the Overview Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Total Web Proxy Activity	You can view the web proxy activity that is being reported by the Secure Web Appliances that are currently managed by the Security Management appliance. This section displays the actual number of transactions and the approximate date that the activity occurred in graphical format. You can also view the percentage of web proxy activity that are suspect, or clean proxy activity, including the total number of transactions.
Suspect Transactions	You can view the web transactions that have been labeled as suspect by the administrator in a graphical format. This section displays the actual number of transactions and the approximate date that the activity occurred, in graphical format. You can also view the percentage of blocked or warned transactions that are suspect. Additionally you can see the type of transactions that have been detected and blocked, and the actual number of times that this transaction was blocked.
L4 Traffic Monitor Summary	You can view any L4 traffic that is being reported by the Secure Web Appliances that are currently managed by the Security Management appliance, in graphical format.
Top URL Categories: Total Transactions	You can view the top URL categories that are being blocked, including the type of URL category and the actual number of times the specific type of category has been blocked in graphical format. The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 37.
Top Application Types: Total Transactions	You can view the top application types that are being blocked, including the name of the actual application type and the number of times the specific application has been blocked, in graphical format.
Top Malware Categories: Monitored or Blocked	You can view all the Malware categories that have been detected, in graphical format.

Section	Description
Top Users: Blocked or Warned Transactions	You can view the actual users that are generating the blocked or warned transactions, in graphical format. Users can be displayed by IP address or by user name.
Top Threat Categories: Blocked by WBRS	You can view all the threat categories that have been blocked, in graphical format

Application Visibility Page



Note For detailed information on Application Visibility, see the 'Understanding Application Visibility and Control' topic in User Guide for AsyncOS for Cisco Secure Web Appliance.

The **Application Visibility** report page allows you to apply controls to particular application types within the Security Management appliance and Secure Web Appliance.

To view the Application Visibility report page, choose **Monitoring > Application Visibility** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

The application control gives you more granular control over web traffic than just URL filtering, for example, as well as more control over the following types of applications, and application types:

- Evasive applications, such as anonymizers and encrypted tunnels.
- Collaboration applications, such as Cisco WebEx, Facebook, and instant messaging.
- Resource intensive applications, such as streaming media.

Understanding the Difference between Application versus Application Types

It is crucial to understand the difference between an application and an application types so that you can control the applications involved for your reports.

- **Application Types**. A category that contains one or more applications. For example, search engines is an application type that may contain search engines such as Google Search and Craigslist. Instant messaging is another application type category which may contain Yahoo Instant Messenger, or Cisco WebEx. Facebook is also an application type.



Note Not all the application types of AVC is applicable for ADC.

- **Applications**. Particular applications that belong in an application type. For example, YouTube is an application in the Media application type.
- **Application behaviors**. Particular actions or behaviors that users can accomplish within an application. For example, users can transfer files while using an application, such as Yahoo Messenger. Not all applications include application behaviors you can configure.

From the Application Visibility page, you can view the following information:

Table 5: Details on the Application Visibility Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Top Application Types by Total Transactions	You can view the top application types that are being visited on the site in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49. For example, instant messaging tools such as Yahoo Instant Messenger, Facebook, and Presentation application types.
Top Applications by Blocked Transactions	You can view the top application types that triggered a block action to occur per transaction in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49. For example, a user has tried to start a certain application type, for example Google Talk or Yahoo Instant Messenger, and because of a specific policy that is in place, this triggered a block action. This application then gets listed in this graph as a transaction blocked or warning.
Application Types Matched	The Application Types Matched interactive table allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions table. From the Applications column you can click on an application to view details.
Applications Matched	The Applications Matched interactive table shows all the application during a specified time range. Additionally, you can find a specific Application within the Application Matched section. In the text field at the bottom of this section, enter the specific Application name and click Find Application.

Layer 4 Traffic Monitor Page

The **Layer 4 Traffic Monitor** report page displays information about malware ports and malware sites that the Layer 4 Traffic Monitors on your Secure Web Appliances have detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

To view the Web Sites report page, choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

The Layer 4 Traffic Monitor listens to network traffic that comes in over all ports on each Secure Web Appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

You can use data in this report to determine whether to block a port or a site, or to investigate why a particular client IP address is connecting unusually frequently to a malware site (for example, this could be because the computer associated with that IP address is infected with malware that is trying to connect to a central command and control server.)

Table 6: Details on the Layer 4 Traffic Monitor Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Top Client IPs: Malware Connections Detected	You can view the top IP addresses of computers in your organization that most frequently connect to malware sites, in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see Choosing Which Data to Chart , on page 5. This chart is the same as the "Layer 4 Traffic Monitor: Malware Connections Detected" chart on the Client Malware Risks Page, on page 47.
Top Malware Sites: Malware Connections Detected	You can view the top malware domains detected by the Layer 4 Traffic Monitor, in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see Choosing Which Data to Chart , on page 5.
Client Source IPs	You can use the this interactive table to view the IP addresses of computers in your organization that frequently connect to malware sites. To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Client IP. You can use this feature to help determine which ports are used by malware that "calls home" to malware sites. To view details such as the port and destination domain of each connection, click an entry in the table. For example, if one particular client IP address has a high number of Malware Connections Blocked, click the number in that column to view a list of each blocked connection. The list is displayed as search results in the Layer 4 Traffic Monitor tab of the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 54. This chart is the same as the "Layer 4 Traffic Monitor: Malware Connections Detected" chart on the Client Malware Risks Page, on page 47.

Section	Description
Malware Ports	You can use the this interactive table to view the ports on which the Layer 4 Traffic Monitor has most frequently detected malware. To view details, click an entry in the table. For example, click the number of Total Malware Connections Detected to view details of each connection on that port. The list is displayed as search results in the Layer 4 Traffic Monitor tab on the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 54.
Malware Sites Detected	You can use the this interactive table to view the domains on which the Layer 4 Traffic Monitor most frequently detects malware. To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Port. You can use this feature to help determine whether to block a site or a port. To view details, click an entry in the table. For example, click the number of Malware Connections Blocked to view the list of each blocked connection for a particular site. The list is displayed as search results in the Layer 4 Traffic Monitor tab on the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 54.

Related Topics

Troubleshooting L4 Traffic Monitor Reports , on page 11

SOCKS Proxy Page

The SOCKS Proxy report page allows you to view transactions processed through the SOCKS proxy, including information about destinations and users, in a graphical and tabular format.

To view the SOCKS Proxy report page, choose **Monitoring > SOCKS Proxy** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.



Note The destination shown in the report is the address that the SOCKS client (typically a browser) sends to the SOCKS proxy.

To change SOCKS policy settings, see *User Guide for AsyncOS for Cisco Secure Web Appliances*.

Table 7: Details on the SOCKS Proxy Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.

Section	Description
Top Destinations for SOCKS: Total Transactions	You can view the top destinations detected by the SOCKS proxy, in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Top Users for SOCKS: Malware Transactions	You can view the top users detected by the SOCKS proxy, in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Destinations	You can use the this interactive table to view the list of destination domains or IP addresses processed through SOCKS proxy. To include only data for a particular destination, enter a domain name or IP address into the box at the bottom of the table and click **Find Domain or IP**.
Users	You can use the this interactive table to view the list of users or IP addresses processed through SOCKS proxy. To include only data for a particular user, enter a user name or IP address into the box at the bottom of the table and click **Find User ID / Client IP Address**.

Related Topics

Searching for Transactions Processed by the SOCKS Proxy , on page 54

URL Categories Page

The **URL Categories** report page can be used to view the URL categories of sites that users on your system are visiting.

To view the URL Categories report page, choose **Monitoring > URL Categories** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

From the URL Categories page, you can view the following information:

Table 8: Details on the URL Categories Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.

Section	Description
Top URL Categories: Total Transactions	You can view the top URL Categories that are being visited on the site in a graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Top URL Categories: Blocked and Warned Transactions	You can view the top URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain URL and because of a specific policy that is in place, this triggered a block action or a warning. This URL then gets listed in this graph as a transaction blocked or warning. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Top Youtube Categories : Total Transactions	You can view the top Youtube Categories that are being visited on the site in a graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Top Youtube Categories : Blocked and Warned Transactions	You can view the top Youtube URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain Youtube URL and because of a specific policy that is in place, this triggered a block action or a warning. This Youtube URL then gets listed in this graph as a transaction blocked or warning. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
URL Categories Matched	The URL Categories Matched interactive table shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category. If there are a large number of unclassified URLs, see Reducing Uncategorized URLs , on page 36.

Reducing Uncategorized URLs

If the percentage of uncategorized URLs is higher than 15-20%, consider the following options:

- For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. These transactions will then be included in “URL Filtering Bypassed” statistics instead. To do this, see information about custom URL categories AsyncOS for Cisco Secure Web Appliances User Guide.

- For sites that you feel should be included in existing or other categories, see Reporting Misclassified and Uncategorized URLs , on page 37.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated automatically on your Secure Web Appliance.

When these updates occur, old category names will continue to appear in reports until the data associated with the older categories is too old to be included in reports. Report data generated after a URL category set update will use the new categories, so you may see both old and new categories in the same report.

Using The URL Categories Page in Conjunction with Other Reporting Pages

The URL Categories page can be used in conjunction with the Application Visibility Page, on page 31, the User Details Page (Web Reporting) , on page 40and the Users Page, on page 38 to investigate a particular user and the types of applications or websites that a particular user is trying to access.

For example, from the URL Categories Page, on page 35, you can generate a high level report for Human Resources which details all the URL categories that are visited by the site. From the same page, you can gather further details in the URL Categories interactive table about the URL category 'Streaming Media'. By clicking on the Streaming Media category link, you can view the specific URL Categories report page. This page not only displays the top users that are visiting streaming media sites (in the Top Users by Category for Total Transactions section), but also displays the domains that are visited (in the Domains Matched interactive table) such as YouTube.com or QuickPlay.com.

At this point, you are getting more and more granular information for a particular user. Now, let's say this particular user stands out because of their usage, and you want to find out exactly what they are accessing. From here you can click on the user in the Users interactive table. This action takes you to the Users Page, on page 38, where you can view the user trends for that user, and find out exactly what they have been doing on the web.

If you wanted to go further, you can now get down to web tracking details by clicking on Transactions Completed link in the interactive table. This displays the Searching for Transactions Processed by Web Proxy Services, on page 50 on the Web Tracking page where you can see the actual details about what dates the user accessed the sites, the full URL, the time spent on that URL, etc.

Reporting Misclassified and Uncategorized URLs

You can report misclassified and uncategorized URLs at the following URL:

https://talosintelligence.com/tickets.

Submissions are evaluated for inclusion in subsequent rule updates.

To check the status of submitted URLs, click the **Status on Submitted URLs** tab on this page.

HTTPS Reports Page

The HTTPS Reports report page is an overall aggregation of the HTTP/HTTPS traffic summary (transactions or bandwidth usage) on the managed appliances.

You can also view the summary of supported ciphers based on either client side connections or server side connections, for individual HTTP/HTTPS web traffic that passes through the managed appliance.

To view the HTTPS Reports report page, choose **Monitoring > HTTPS Reports** from the **Reports** drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

Table 9: Details on the HTTPS Reports Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Changing the Time Range, on page 3.
Web Traffic Summary	You can view the web traffic summary on the appliance in one of the following ways: • **Transactions**: Select this option from the drop-down list to display the web traffic summary based on the number of HTTP or HTTPS web transactions, in a graphical format and percentage of HTTP or HTTPS web transaction in tabular format. • **Bandwidth Usage**: Select this option from the drop-down list to display the web traffic summary based on the amount of bandwidth consumed by the HTTP or HTTPS web traffic, in a graphical format and the percentage of HTTP or HTTPS bandwidth usage in tabular format.
Trend: Web Traffic	You can view the trend graph for the web traffic on the appliance based on the required time range in one of the following ways: • **Web Traffic Trend**: Select this option from the dropdown list to display the cumulative trend for HTTP and HTTPS web traffic based on the transactions or bandwidth usage. • **HTTPS Trend**: Select this option from the dropdown list to display the trend for HTTPS web traffic based on the transactions or bandwidth usage. • **HTTP Trend**: Select this option from the dropdown list to display the trend for HTTP web traffic based on the transactions or bandwidth usage.
Ciphers	You can view the summary of the ciphers in one of the following ways: • **By Client Side Connections**: Select this option from the dropdown list to display the summary of the ciphers used on the client side of the HTTP or HTTPS web traffic in a graphical format. • **By Server Side Connections**: Select this option from the dropdown list to display the summary of the ciphers used on the server side of the HTTP or HTTPS web traffic in a graphical format.

Users Page

The **Users** report page provides several links that allow you to view web reporting information for individual users.

To view the Users report page, choose **Monitoring > Users** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

From the **Users** page you can view how long a user, or users, on your system have spent on the internet, on a particular site or URL, and how much bandwidth that user is using.

Note The maximum number of users on the Secure Web Appliance that the Security Management appliance can support is 500.

From the **Users** page, you can view the following information pertaining to the users on your system:

Table 10: Details on the Users Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Top Users: Transactions Blocked	You can view the top users, by either IP address or user name, and the number of transactions that have been blocked specific to that user, in graphical format. The user name or IP address can be made unrecognizable for reporting purposes. For more information on how to make user names unrecognizable in for this page or in scheduled reports, see the *User Guide for AsyncOS for Cisco Content Security Management Appliances*. The default setting is that all user names appear. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Top Users: Bandwidth Used	You can view the top users, by either IP address or user name, that are using the most bandwidth on the system, in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Users	You can use this interactive table to search for a specific User ID or Client IP address. In the text field at the bottom of the User table, enter the specific User ID or Client IP address and click on Find User ID / Client IP Address. The IP address does not need to be an exact match to return results. You can click on a specific user to find more specific information. For more information, see the User Details Page (Web Reporting) , on page 40

Note To view user IDs instead of client IP addresses, you must set up your Security Management appliance to obtain user information from an LDAP server.

User Details Page (Web Reporting)

The **User Details** page allows you to see specific information about a user that you have identified in the interactive table on the Users report page.

The User Details page allows you to investigate individual user's activity on your system. This page is particularly useful if you are running user-level investigations and need to find out, for example, what sites your users are visiting, what Malware threats they are encountering, what URL categories they are accessing, and how much time a specific user is spending at these sites.

To display the User Details page for a specific user, click on a specific user from the Users interactive table on the **Users** report page.

From the User Details page, you can view the following information pertaining to an individual user on your system:

Table 11: Details on the User Details Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
URL Categories: Total Transactions	You can view the specific URL Categories that a specific user is using, in graphical format. To customize the view of the chart, click ✓ on the chart. The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 16.
Trend: Total Transactions	You can use this trend graph to view all the web transactions of a specific user. To customize the view of the chart, click ✓ on the chart. For example, this graph will indicate if there is a large spike in web traffic during certain hours of the day, and when those spikes occur. Using the Time Range drop-down list, you can expand this graph to see a more or less granular span of time that this user was on the web.
URL Categories Matched	The URL Categories Matched interactive table shows matched categories for both completed and blocked transactions. You can search for a specific URL Category in the text field at the bottom of the table and click **Find URL Category**. The category does not need to be an exact match. The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 16.

Section	Description
Domains Matched	The Domains Matched interactive table shows domains or IP addresses that the user has accessed. You can also view the time spent on those categories, and various other information that you have set from the column view. You can search for a specific Domain or IP address in the text field at the bottom of the table and click **Find Domain or IP**. The domain or IP address does not need to be an exact match.
Applications Matched	The Applications Matched interactive table shows applications that a specific user is using. For example, if a user is accessing a site that requires use of a lot of Flash video, you will see the application type in the Application column. You can search for a specific application name in the text field at the bottom of the table and click **Find Application**. The name of the application does not need to be an exact match.
Advanced Malware Protection Threats Detected	The Advanced Malware Protection Threats Detected interactive table shows malware threat files that are detected by the Advanced Malware Protection engine. You can search for data on a specific SHA value of the malware threat file, in the text field at the bottom of the table and click **Find malware Threat File SHA 256**. The name of the application does not need to be an exact match.
Malware Threats Detected	The Malware Threats Detected interactive table shows the top Malware threats that a specific user is triggering. You can search for data on a specific malware threat name in the text field at the bottom of the table and click **Find Malware Threat**. The name of the Malware Threat does not need to be an exact match.
Policies Matched	The Policies Matched interactive table shows the policy groups that applied to this user when accessing the web. You can search for a specific policy name in the text field at the bottom of the table and click **Find Policy**. The name of the policy does not need to be an exact match.



Note From Client Malware Risk Details table: The client reports sometimes show a user with an asterisk (*) at the end of the user name. For example, the Client report might show an entry for both “jsmith” and “jsmith*”. User names listed with an asterisk (*) indicate the user name provided by the user, but not confirmed by the authentication server. This happens when the authentication server was not available at the time and the appliance is configured to permit traffic when authentication service is unavailable.

Web Sites Page

The **Web Sites** report page is an overall aggregation of the activity that is happening on the managed appliances. You can use this report page to monitor high-risk web sites accessed during a specific time range.

To view the Web Sites report page, choose **Monitoring** > **Web Sites** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

From the Web Sites page, you can view the following information:

Table 12: Details on the Web Sites Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Top Domains: Total Transactions	You can view the top domains that are being visited on the website in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Top Domains: Transactions Blocked	You can view the top domains that triggered a block action to occur per transaction in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49. For example, a user went to a certain domain and because of a specific policy that I have in place, this triggered a block action. This domain is listed in this graph as a transaction blocked, and the domain site that triggered the block action is listed.
Domains Matched	You can use this interactive table to search for the domains that are that are being visited on the website. You can click on a specific domain to access more granular information. The Proxy Services tab on the Web Tracking page appears and you can see tracking information and why certain domains were blocked. When you click on a specific domain you can see the top users of that domain, the top transactions on that domain, the URL Categories matched and the Malware threats that have been detected.

Advanced Malware Protection Page

Advanced Malware Protection protects against zero-day and targeted file-based threats by:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.

- Evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

For more information on the file reputation filtering and file analysis, see the user guide or online help for *AsyncOS for Secure Web Appliances*.

The Advanced Malware Protection report page shows the following reporting views:

- Advanced Malware Protection–Summary Page
- Advanced Malware Protection–File Analysis Page

To view the Advanced Malware Protection report page, choose **Monitoring > Advanced Malware Protection** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

Advanced Malware Protection - AMP Summary Page

The AMP Summary section of the Advanced Malware Protection report page shows file-based threats that were identified by the file reputation service.

To see the users who tried to access each SHA, and the filenames associated with that SHA-256, click a SHA-256 in the table.

You can click on the link in the Malware Threat Files interactive table to view all the instances of the file in Web Tracking that were encountered within the maximum available time range, regardless of the time range selected for the report.

If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.

You can use the AMP Summary section of the Advanced Malware Protection page to view:

- The summary of files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- The top malware threat files in a graphical format.
- The top threat files based on the file types in a graphical format.
- A trend graph for all the malware threat files based on the selected time range.
- The Malware Threat Files interactive table that lists the top malware threat files.
- The Files With Retrospective Verdict Change interactive table that lists the files processed by this appliance for which the verdict has changed since the transaction was processed. For more information about this situation, see the documentation for your Secure Web Appliance.

  In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.

  If multiple Secure Web Appliances have different verdict updates for the same file, the result with the latest time stamp is displayed.

  You can click on a SHA-256 link to view web tracking results for all transactions that included this SHA-256 within the maximum available time range, regardless of the time range selected for the report.

Advanced Malware Protection - File Analysis Page

The File Analysis section of the Advanced Malware Protection report page shows the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.

For deployments with an on-premises Cisco AMP Malware Analytics Appliance: Files that are on the allowed list on the Cisco AMP Malware Analytics appliance show as "clean." For information about allowed listing, see the AMP Malware Analytics online help.

Drill down to view detailed analysis results, including the threat characteristics and score for each file.

You can also view additional details about an SHA directly on the server that performed the analysis by searching for the SHA or by clicking the Cisco AMP Malware Analytics link at the bottom of the file analysis details page.

If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.

You can use the File Analysis section of the Advanced Malware Protection report page to view:

- The number of files that are uploaded for file analysis by file analysis service of the Advanced Malware Protection engine.
- A list of files that have completed file analysis requests.
- A list of files that have pending file analysis requests.

Anti-Malware Page

The **Anti-Malware** report page is a security-related reporting page that reflects the results of scanning by your enabled scanning engines (Webroot, Sophos, McAfee, and/or Adaptive Scanning).

To view the Anti-Malware report page, choose **Monitoring > Anti-Malware** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

You can use this page to help identify and monitor web-based malware threats.



Note To view data for malware found by L4 Traffic Monitoring, see Layer 4 Traffic Monitor Page, on page 32

From the Anti-Malware page, you can view the following information:

Table 13: Details on the Anti-Malware Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Top Malware Categories	You can view the top malware categories that are detected by a given category type, in graphical format. See Malware Category Descriptions, on page 45 for more information on valid Malware categories. To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.

Section	Description
Top Malware Threats	You can view the the top malware threats in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49.
Malware Categories	The Malware Categories interactive table shows detailed information about particular malware categories that are displayed in the Top Malware Categories chart. Clicking on any of the links in the Malware Categories interactive table allows you to view more granular details about individual malware categories and where they are on the network. Exception: an Outbreak Heuristics link in the table lets you view a chart showing when transactions in this category occurred. See Malware Category Descriptions, on page 45 for more information on valid Malware categories.
Malware Threats	The Malware Threats interactive table shows detailed information about particular malware threats that are displayed in the Top Malware Threats section. Threats labeled “Outbreak” with a number are threats identified by the Adaptive Scanning feature independently of other scanning engines.

Malware Category Report Page

Procedure

Step 1 Choose **Reporting** > **Anti-Malware**.

Step 2 In the Malware Categories interactive table, click on a category in the Malware Category column.

Malware Threat Report

The Malware Threat Report page shows clients at risk for a particular threat, displays a list of potentially infected clients, and links to the Client Detail page. The trend graph at the top of the report shows monitored and blocked transactions for a threat during the specified time range. The table at the bottom shows the actual number of monitored and blocked transactions for a threat during the specified time range.

To view this report, click a category in the Malware Category column of the Anti-Malware report page.

For additional information, click the **Support Portal Malware Details** link below the table.

Malware Category Descriptions

The Secure Web Appliance can block the following types of malware:

Malware Type	Description
Adware	Adware encompasses all software executables and plug-ins that direct users towards products for sale. Some adware applications have separate processes that run concurrently and monitor each other, ensuring that the modifications are permanent. Some variants enable themselves to run each time the machine is started. These programs may also change security settings making it impossible for users to make changes to their browser search options, desktop, and other system settings.
Browser Helper Object	A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	A dialer is a program that utilizes your modem or another type of Internet access to connect you to a phone line or a site that causes you to accrue long distance charges to which you did not provide your full, meaningful, and informed consent.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	A hijacker modifies system settings or any unwanted changes to a user's system that may direct them to a website or run a program without a user's full, meaningful, and informed consent.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Outbreak Heuristics	This category represents malware found by Adaptive Scanning independently of the other anti-malware engines.
Phishing URL	A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following actions: Overtly or covertly records system processes and/or user action. Makes those records available for retrieval and review at a later time.
Trojan Downloader	A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host. These installations usually occur without the user's knowledge. Additionally, a Trojan Downloader's payload may differ from installation to installation since it obtains downloading instructions from the remote host/site.
Trojan Horse	A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.

Malware Type	Description
Trojan Phisher	A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passwords for bank sites, auction sites, or online payment sites.
Virus	A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
Worm	A worm is program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Client Malware Risks Page

The **Reporting > Client Malware Risk** page is a security-related reporting page that can be used to monitor client malware risk activity. The Client Malware Risk page also lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM).

Table 14: Details on Client Malware Risks Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Web Proxy: Top Clients Monitored or Blocked	This chart displays the top ten users that have encountered a malware risk.
L4 Traffic Monitor: Malware Connections Detected	This chart displays the IP addresses of the computers in your organization that most frequently connect to malware sites.
Web Proxy: Client Malware Risk	The Web Proxy: Client Malware Risk interactive table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section.
L4 Traffic Monitor: Clients by Malware Risk	The L4 Traffic Monitor: Clients by Malware Risk interactive table displays IP addresses of computers in your organization that frequently connect to malware sites.

Web Reputation Filters Page

You can use the **Web Reputation Filters** report page to view the results of your set Web Reputation filters for transactions during a specified time range.

To view the Web Reputation Filters report page, choose **Monitoring > Web Reputation Filters** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 8.

What are Web Reputation Filters?

Web Reputation Filters analyze web server behavior and assign a reputation score to a URL to determine the likelihood that it contains URL-based malware. It helps protect against URL-based malware that threatens end-user privacy and sensitive corporate information. The Secure Web Appliance uses URL reputation scores

to identify suspicious activity and stop malware attacks before they occur. You can use Web Reputation Filters with both Access and Decryption Policies.

Web Reputation Filters use statistical data to assess the reliability of Internet domains and score the reputation of URLs. Data such as how long a specific domain has been registered, or where a web site is hosted, or whether a web server is using a dynamic IP address is used to judge the trustworthiness of a given URL.

The web reputation calculation associates a URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a Web Reputation Score between -10 and +10, with +10 being the least likely to contain malware.

Example parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on any block lists
- Presence on any allow lists
- URL typos of popular domains
- Domain registrar information
- IP address information

For more information on Web Reputation Filtering, see 'Web Reputation Filters' in the *User Guide for AsyncOS for Secure Web Appliances*.

From the Web Reputation Filters page, you can view the following information:

Table 15: Details on Web Reputation Filters Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 4.
Web Reputation Actions (Trend)	You can view the total number of web reputation actions against the time specified, in graphical format. From this you can see potential trends over time for web reputation actions.
Web Reputation Actions (Volume)	You can view the web reputation action volume in percentages by transactions.

Section	Description
Web Reputation Threat Types Blocked by WBRS	You can view the types of threats found in transactions that were blocked by Web Reputation filtering, in graphical format. **Note** WBRS cannot always identify the threat type.
Threat Types Detected in Other Transactions	You can view the type of threats found in transactions that were not blocked by Web Reputation filtering, in graphical format. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 49. Reasons these threats might not have been blocked include: • Not all threats have a score that meets the threshold for blocking. However, other features of the appliance may catch these threats. • Policies might be configured to allow threats to pass through. **Note** WBRS cannot always identify the threat type.
Web Reputation Actions (Breakdown by Score)	If Adaptive Scanning is not enabled, this interactive table displays the Web Reputation scores broken down for each action.
Threat Categories Matched	You can view the threat categories matched, in graphical format.

Adjusting Web Reputation Settings

Based on your report results, you may want to adjust the configured web reputation settings, for example adjust the threshold scores or enable or disable Adaptive Scanning. For specific information about configuring web reputation settings, see *User Guide for AsyncOS for Cisco Secure Web Appliances*.

(Web Reports Only) Choosing Which Data to Chart

The default charts on each Web Reporting page display commonly-referenced data, but you can choose to chart different data instead. If a page has multiple charts, you can change each chart.

Generally, the chart options are the same as the columns of the table in the report. However, some columns cannot be charted.

Charts reflect all available data in a table column, regardless of the number of items (rows) you choose to display in the associated table.

Procedure

Step 1 Click ✓ on a specific chart.

Step 2 Choose the required data to be displayed. The preview of the chart is displayed as per the selected options.

Step 3 Click **Apply**.

Web Tracking on the New Web Interface

You can use the **Web Tracking Search** page to search and view details about individual transactions or patterns of transactions that may be of concern. Depending on the services that your deployment uses, search in relevant tabs:

- Searching for Transactions Processed by Web Proxy Services, on page 50
- Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 54
- Searching for Transactions Processed by the SOCKS Proxy , on page 54
- Working with Web Tracking Search Results , on page 55
- Viewing Transaction Details for Web Tracking Search Results , on page 56

For more information about the distinction between the Web Proxy and the Layer4 Traffic Monitor, see the "Understanding How the Secure Web Appliance Works" section in *User Guide for AsyncOS for Cisco Secure Web Appliances.*

Searching for Transactions Processed by Web Proxy Services

You can use the **Proxy Services** tab on the **Web Tracking Search** page to search web tracking data aggregated from individual security components and acceptable use enforcement components. This data does not include Layer 4 Traffic Monitoring data or transactions processed by the SOCKS Proxy.

You might want to use it to assist the following roles:

- **HR or Legal manager.** Run an investigative report for an employee during a specific time period.

  For example, you can use the Proxy Services tab to retrieve information about a specific URL that a user is accessing, what time the user visited that URL, whether that URL is allowed, etc.

- **Network security administrator.** Examine whether the company network is being exposed to malware threats through employees' smartphones.

You can view search results for the transactions recorded (including blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.



Note The Web Proxy only reports on transactions that include an ACL decision tag other than "OTHER-NONE.

For an example of how the Proxy Services tab can be used with other web reporting pages, see the .

Procedure

Step 1 On the Security Management appliance, choose **Web** from the dropdown list..

Step 2 Using The URL Categories Page in Conjunction with Other Reporting Pages, on page 37 Choose **Tracking** > **Proxy Services**.

Step 3 To see all search and filtering options, click **Advanced**.

Step 4 Enter search criteria:

Table 16: Web Tracking Search Criteria on the Proxy Services Tab

Option	Description
Default Search Criteria	
Time Range	Choose the time range on which to report. For information on time ranges available on the Security Management appliance, see the Choosing a Time Range for Reports, on page 4.
User/Client IPv4 or IPv6	Optionally, enter an authentication username as it appears in reports or a client IP address that you want to track. You can also enter an IP range in CIDR format, such as 172.16.0.0/16. When you leave this field empty, the search returns results for all users.
Website	Optionally, enter a website that you want to track. When you leave this field empty, the search returns results for all websites.
Transaction Type	Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.
Advanced Search Criteria	
URL Category	To filter by a URL category, select **Filter by URL Category** and type the first letter of a custom or predefined URL category by which to filter. Choose the category from the list that appears . All recent transactions that match the category name are included, regardless of the engine name noted in the drop-down list.
Malware Threat	To filter by a particular malware threat, select **Filter by Malware Threat** and enter a malware threat name by which to filter. To filter by a malware category, select **Filter by Malware Category** and choose a malware category by which to filter. For descriptions, see Malware Category Descriptions, on page 45.
Application	To filter by an application, select **Application** and choose an application by which to filter. To filter by an application type, select **Application Type** and choose an application type by which to filter.

Option	Description
WBRS	In the WBRS section, you can filter by Web-Based Reputation Score and by a particular web reputation threat. • To filter by web reputation score, select **Score Range**and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting **No Score**. • To filter by web reputation threat, select **Filter by Reputation Threat** and enter a web reputation threat by which to filter. For more information on WBRS scores, see the IronPort AsyncOS for Web User Guide.
Threat Category	To filter by a specific threat category, expand the **Threat Category** section and select the threat categories that you want. To select all available threat categories, click **Select All**.
Youtube Category	To filter by a specific Youtube category, expand the **Youtube Category** section and select the Youtube categories that you want to view. To select all available Youtube categories, click **Select All**. You can also filter by Acitve and Inactive categories.
Policy	To filter by a policy group, select **Policy** and enter a policy group name by which to filter. Make sure that you have declared the policy on the Secure Web Appliance.
AnyConnect Secure Mobility	To filter by remote or local access, select **User Location** and choose an access type. To include all access types, select **Disable Filter**. (In previous releases, this option was labeled Mobile User Security.)
Advanced Malware Protection	To filter file-based threats identified by the file reputation service, enter a filename in the **Filename** box. To filter files using the SHA-256 hash, enter a SHA-256 has value in the **File SHA-256** box. To filter files based on file verdict, select AMP **File Verdict** and choose a verdict type. The available file verdict types are **Clean**, **Malicious**, **Unknown**, **UnScannable**, and **Lowrisk**. The **Malicious** verdict type has three sub-cateogries: • **Malware**: Files that are blocked due to reasons other than Custom Detection nor Custom Threshold. • **Custom Detection**: The percentage of file SHAs on the blocked list received from the AMP for Endpoints console. • **Custom Threshold**: The files blocked due to Threshold Settings while configuring AMP.

Option	Description
User Request	To filter by transactions that were actually initiated by the user, select **Filter by Web User-Requested Transactions**. **Note:** When you enable this filter, the search results include “best guess” transactions.

Malware Category Descriptions

The Secure Web Appliance can block the following types of malware:

Malware Type	Description
Adware	Adware encompasses all software executables and plug-ins that direct users towards products for sale. Some adware applications have separate processes that run concurrently and monitor each other, ensuring that the modifications are permanent. Some variants enable themselves to run each time the machine is started. These programs may also change security settings making it impossible for users to make changes to their browser search options, desktop, and other system settings.
Browser Helper Object	A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	A dialer is a program that utilizes your modem or another type of Internet access to connect you to a phone line or a site that causes you to accrue long distance charges to which you did not provide your full, meaningful, and informed consent.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	A hijacker modifies system settings or any unwanted changes to a user’s system that may direct them to a website or run a program without a user’s full, meaningful, and informed consent.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Outbreak Heuristics	This category represents malware found by Adaptive Scanning independently of the other anti-malware engines.
Phishing URL	A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.

Malware Type	Description
System Monitor	A system monitor encompasses any software that performs one of the following actions: Overtly or covertly records system processes and/or user action. Makes those records available for retrieval and review at a later time.
Trojan Downloader	A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host. These installations usually occur without the user's knowledge. Additionally, a Trojan Downloader's payload may differ from installation to installation since it obtains downloading instructions from the remote host/site.
Trojan Horse	A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.
Trojan Phisher	A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passwords for bank sites, auction sites, or online payment sites.
Virus	A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
Worm	A worm is program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Searching for Transactions Processed by the Layer 4 Traffic Monitor

The Layer 4 Traffic Monitor tab on the **Web Tracking Search** page provides details about connections to malware sites and ports. You can search for connections to malware sites by the following types of information:

- Time range
- IP address of the machine that initiated the transaction (IPv4 or IPv6)
- Domain or IP address of the destination website (IPv4 or IPv6)
- Port
- IP address associated with a computer in your organization
- Connection type

To view the hostname at the questionable site or the Secure Web Appliance that processed the transaction, click the Display Details link in the Destination IP Address column heading.

For more information about how you can use this information, see Layer 4 Traffic Monitor Page, on page 32.

Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; IP address of the client machine that initiated the transaction; and destination domain, IP address, or port. You can also filter results by custom URL category, policy matched, and user location (local or remote). IPv4 and IPv6 addresses are supported.

Procedure

Step 1 Choose **Tracking** > **SOCKS Proxy**.

Step 2 To see all search and filtering options, click **Advanced**.

Step 3 Enter search criteria.

Step 4 Click **Search**.

What to do next

Related Topics

SOCKS Proxy Page, on page 34

Working with Web Tracking Search Results

- Displaying More Web Tracking Search Results , on page 55
- Understanding Web Tracking Search Results , on page 55
- Viewing Transaction Details for Web Tracking Search Results , on page 56
- About Web Tracking and Upgrades , on page 56

Displaying More Web Tracking Search Results

Procedure

Step 1 Be sure to review all pages of returned results.

Step 2 To display more results per page than the current number displayed, select an option from the **Items Displayed** menu.

Step 3 If more transactions match your criteria than the maximum number of transactions offered in the Items Displayed menu, you can view the complete set of results by clicking the **Printable Download** link to obtain a CSV file that includes all matching transactions.

This CSV file includes the complete set of raw data, excluding details of related transactions.

Understanding Web Tracking Search Results

By default, results are sorted by time stamp, with the most recent result at the top.

Search results include:

- The time that the URL was accessed.
- The number of related transactions spawned by the user-initiated transaction, such as images loaded, javascripts run, and secondary sites accessed. The number of related transactions appears in each row below the Display All Details link in the column heading.

- The disposition (The result of the transaction. If applicable, shows the reason the transaction was blocked, monitored, or warned.)

Viewing Transaction Details for Web Tracking Search Results

To View	Do This
The full URL for a truncated URL in the list	Note which host Secure Web Appliance processed the transaction, then check the Accesslog on that appliance.
Details for an individual transaction	Click a URL in the Website column.
Details for all transactions	Click the **Display All Details...** link in the Website column heading.
A list of up to 500 related transactions	The number of related transactions appears in parentheses below the "Display Details" link in the column heading in the list of search results. Click the **Related Transactions** link in the Details view for a transaction.

About Web Tracking and Upgrades

New web tracking features may not apply to transactions that occurred before upgrade, because the required data may not have been retained for those transactions. For possible limitations related to web tracking data and upgrades, see the Release Notes for your release.

Scheduling and Archiving Web Reports on the New Web Interface

This section includes the following:

- Scheduling Web Reports on the New Web Interface, on page 56
- Archiving Web Reports on the New Web Interface, on page 58

Scheduling Web Reports on the New Web Interface

This section includes the following:

- Adding Scheduled Web Reports on the New Web Interface, on page 57
- Editing Scheduled Web Reports on the New Web Interface, on page 57
- Deleting Scheduled Web Reports on the New Web Interface, on page 57

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, previous month, previous calendar day (up to 250), previous calendar month (up to 12). Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months).

Regardless of when you run a report, the data is returned from the previous time interval (hour, day, week, or month). For example, if you schedule a daily report to run at 1AM, the report will contain data from the previous day, midnight to midnight (00:00 to 23:59).

You can define as many recipients for reports as you want, including zero recipients. If you do not specify an email recipient, the system will still archive the reports. If you need to send the reports to a large number of addresses, however, you may want to create a mailing list instead of listing the recipients individually.

Adding Scheduled Web Reports on the New Web Interface

Procedure

Step 1 Choose **Monitoring > Schedule & Archive**.

Step 2 In the Schduled / Archived tab, click the + button.

Step 3 Select your report type from the **Report Type** drop-down menu.

Step 4 In the **Report Title** field, enter the title of your report.

To avoid creating multiple reports with the same name, we recommend using a descriptive title.

Step 5 Choose the time range for the report from the **Time Range to Include** drop-down menu.

Step 6 Choose the format for the generated report.

The default format is PDF.

Step 7 From the Delivery Options section, choose any one of the following:

By choosing this, the report will be listed on the Archived Reports page.

Note
Domain-Based Executive Summary reports cannot be archived.

- To archive the report, select **Only Archive**.
- To archive and email the report, click **Archive and Email to Recipients**.
- To email the report, click **Only Email to Recipients**.

In the **Email IDs** field, enter the recipient email addresses.

Step 8 From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

Step 9 Select the language in which the report must be generated from the **Report Language** drop-down list.

Step 10 Click **Submit**.

Editing Scheduled Web Reports on the New Web Interface

To edit reports on the new web interface of your appliance, choose **Monitoring > Scheduled & Archive** page. Click on the link corresponding to the Report Title of report that you want to edit. Modify the settings and then click **Edit** to submit your changes on the page.

Deleting Scheduled Web Reports on the New Web Interface

To delete reports on the new web interface of your appliance, choose **Monitoring > Scheduled / Archived** page. Select the checkboxes corresponding to the reports that you want to delete and click on the trash can icon.

To remove all scheduled reports, select the check box next to the report title. Note that archived versions of deleted reports are not deleted.

Archiving Web Reports on the New Web Interface

- [New Web Interface] Generating Web Reports on Demand, on page 58
- Viewing and Managing Archived Web Reports on the New Web Interface, on page 59

[New Web Interface] Generating Web Reports on Demand

Most reports that you can schedule, you can also generate on demand.

To generate a report on demand, perform the following:

Procedure

Step 1 On the Secure Web Appliance, choose **Monitoring > Schedule & Archive**.

Step 2 In the **View Archived** tab, click on the + button.

Step 3 From the **Report Type** section, choose a report type from the drop-down list.

The options on the page may change.

Step 4 In the **Report Title** section, enter the name of the title for the report.

AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.

Step 5 From the **Time Range to Include** drop-down list, select a time range for the report data.

Step 6 In the **Attachment Details** section, choose the format of the report.

PDF. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.

Step 7 From the **Delivery Options** section, choose any one of the following:

By choosing this, the report will be listed on the Archived Reports page.

Note
Domain-Based Executive Summary reports cannot be archived.

- To archive the report, select **Only to Archive**.
- To archive and email the report, click **Archive and Email to Recipients**.
- To email the report, click **Only Email to Recipients**.

In the **Email IDs** field, enter the recipient email addresses.

Step 8 Select the language in which the report must be generated from the **Report Language** drop-down list.

Step 9 Click **Deliver This Report** to generate the report.

Viewing and Managing Archived Web Reports on the New Web Interface

Use the information in this section to work with reports that are generated as scheduled reports.

Procedure

Step 1 Login to the new web interface of your appliance.

Step 2 Select **Monitoring > Schedule& Archive**.

Step 3 Select the **View Archived** tab.

Step 4 To view a report, click the report names in the **Report Title** column. The Report Type drop-down list filters the types of reports that are listed on the **Archived Reports** tab.

Step 5 You can search for a particular report in the search box.

System Status Page on the New Web Interface

On the Secure Web Appliance, choose **Monitoring > System Status** to monitor the System Status. This page displays the current status and configuration of the Secure Web Appliance. Browser time is displayed on the system status page at the top right corner.

The **System Status** page has the following tabs:

- Capacity

The **Status** tab is displayed by default.

Status

The Status page displays the following information.

This Section...	Description
Secure Web Appliance Status	• System uptime • System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging. RAM usage for a system that is working efficiently may be above 90%, because RAM that is not otherwise in use by the system is used by the web object cache. If your system is not experiencing serious performance issues and this value is not stuck at 100%, the system is operating normally. **Note** Proxy Buffer Memory is one component that uses this RAM.

This Section...	Description
Alerts	Displays the alert names and the date and time at which it has occurred. When you click **More** at the top right corner or an alert name, the **All Alerts** pop-up appears. The selected alert row is highlighted in the **All Alerts** pop-up. The **All Alerts** pop-up displays: • Date and Time of Alert • Alert Level - Info, Warning, or Critical • Alert Class • Problem - Short description of the alert • Recipient - email address to which the alert details are sent
Disk Usage	Displays the value of disk usage and RAID storage status. The RAID storage status depends on the appliance configuration. For virtual appliances, the RAID storage status displays "Unknown" and for physical appliances, it displays "Optimal".
Proxy Status	Displays Proxy CPU usage and Proxy Disk I/O utilization. It also displays the proxy connection backlog with the port number and number of connections.
High Availability	Displays the Failover group name, Priority and Status. It also displays the number of High Availability Failover groups enabled. If there are no failover groups, the service status displays "Not Configured".

This Section...	Description

Proxy Traffic Characteristics	Displays the following proxy traffic characteristics:
	• Request Per Second
	• Bandwidth
	• Response Time
	• Cache Hit Rate
	• Current Connections—Number of connections for particular time, and date, and displays details such as:
	  • Idle Client Connections
	  • Idle Server Connections
	  • Total Client Connections
	  • Total Server Connections
	
	It displays the average and maximum values of these data. The average values are shown for the last minute, last hour and since the proxy restart. The maximum values are shown for the last hour and since proxy restart.
	Note
	Click the link icon next to RPS and Bandwidth, that redirects you to the Capacity tab. Similarly, click the link icon next to the Response Time, that redirects you to the Services tab.

Capacity

The Capacity page displays the following information.

This Section...	Description
Time Range	Displays the following Time Range options: • Hour • Day • Week • 30 Days • 90 Days • Yesterday (00:00 to 23:59) • Previous Calendar Month • Custom Range—earliest available data Click **Apply** to view the earliest available data, and click **Cancel** to cancel the operation. **Note** The Time Range option applies to all the features of the Capacity tab.
System CPU and Memory Usage	The System CPU and System Memory Usage allows you to do the following tasks: • Update or set the threshold value (for example, 0-100%). • Change the threshold value. • View the CPU/Memory usage. The color codes are: • Red—Indicates the threshold value. • Green—Indicates the average value. If you change the threshold value, the Average value also gets updated accordingly. The average value is the sum value divided by the length of the records. • Blue—Indicates the system memory usage in percentage. The System CPU and Memory Usage data is displayed in percentage based on the Time Range selection. The data and graph change dynamically based on the current data.
Bandwidth and RPS	Displays the following Bandwidth and RPS details in graphical format: • Overall—Displayed in Dark Blue • HTTPS Decrypted—Displayed in Aqua Blue Click the legend blocks to enable or disable the Overall information and HTTPS Decrypted information.

This Section...	Description
CPU Usage by Function	The color codes for the various CPU Usage options are: • Light Green—Web Proxy • Dark Green—Logging • Purple—Reporting • Yellow—WBRS • Dark Blue— AMP • Light Blue—Webroot • Aqua Blue—Sophos • Grey—McAfee Click the legend blocks to enable or disable the options.
Client or Server Connection	Displays the average and maximum connections, and allows you to do the following tasks: • Enable or disable the average and maximum connections • View the average and maximum connection details and graphs

Services

The Services page displays the services and its status. The services ribbon displays the status of AMP, WCCP, ISE, and CTR services. The color next to the service name denotes the service status:

- Red - The service is not ready.
- Grey - The service is ready, but disabled.
- Green - The service is ready, enabled and running.

This Section...	Description
Date	The service data for the current day is displayed by default. You can view up to previous seven days data. Choose a date from the calendar to view the data for the particular day.

This Section...	Description
Service Status	The Service Status table displays the events and alerts for the services. The table displays a 24-hour time interval, which is divided into 1-hour slots. Each block represents the alerts in a 1-hour time interval. Green color for a block indicates that there are no critical alerts in the corresponding hour. If there is at least one critical alert in an hour, the corresponding block appears in Red color. The blocks corresponding to future time slots is displayed in White. The icon at the left side near the service name displays the color of the last block (or ongoing hour). You can click the Red block to see the times at which the last 5 alerts have occurred. It also displays the total number of alerts as *5 of 'n' Events*, where '*n*' is the total number of alerts occurred during that time period. Click **More** to see the **All Alerts** pop-up. The **All Alerts** pop-up displays: • Date and Time of Alert • Alert Level - Info, Warning, or Critical • Alert Class • Problem - Short description of the alert • Recipient - email address to which the alert details are sent

This Section...	Description
Service Response Time	The Service Response Time table shows the response time pattern taken by each service running in the system. The following times are shown: • McAfee Service Time • WBRS Service Time • DNS Response Time • Webroot Service Time • AMP Service Time • Sophos Service Time • Server Response Time The table displays a 24-hour time interval divided into 1-hour slots. Each block represents the service response pattern in a 1-hour time. The response time for each service is split into the following time slots: • 0.001s to 0.06s • 0.06s to 0.6s • 0.6s to 1s • 1s to 6s • 6s and more By default, the table displays the 1s to 6s response values for all services. You can expand and view the detailed split up. The system calculates the response time for all transactions. It then displays the percentage of transaction volume that has occurred in each timeslot. The block color is based on the transaction volume percentage.

This Section...	Description
	For Response Time below 1 second the transaction volume legend is: • Dark Blue—41% to 100% • Aqua Blue—11% to 40% • Light Blue—1% to 10% • White—0% For Response Time of 1 second and above, the transaction volume legend is: • Red—41% to 100% • Light Red—26% to 40% • Light Blue—1% to 25% • White—0% When the data for Response Time is not available in seconds, the legend color option is white and cannot be edited. Click the Time Range option to retrieve the Service Response Time data. The data includes the bar charts and the number of occurrences. However, you cannot retrieve: • Bar charts • Legend data for previous dates Click a time block to open a pop-up that displays the response trend in bar chart for that particular time. • Horizontal axis—Time slot that is divided into 5-minute intervals • Vertical axis— Number of transactions in the timeslot Hover the mouse over a block in the pop-up to see the number of transactions in that time interval.