Using Centralized Web Reporting and Tracking

This chapter contains the following sections:

Centralized Web Reporting and Tracking Overview

The Cisco Content Security Management appliance aggregates information from security features on multiple Web Security appliances and records data that can be used to monitor your web traffic patterns and security risks. You can run reports in real-time 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. Reporting functionality also allows you to export raw data to a file.

The Centralized Web Reporting feature not only generates high-level reports, allowing administrators to understand what is happening on their network, but it also allows an administrator to drill down and see traffic details for a particular domain, user, or URL category.

Domain

For a domain, the web reporting feature can generate the following data elements to be on a domain report. For example, if you are generating a report on the Facebook.com domain, the report may contain:

• A list of the top users who accessed Facebook.com

• A list of the top URLs that were accessed within Facebook.com

User

For a user, the web reporting feature can generate data elements to be on a user report. For example, for the user report titled 'Jamie', the report may contain:

• A list of the top domains that the user 'Jamie' accessed
• A list of the top URLs that were malware or virus positive
• A list of the top categories that the user 'Jamie' accessed

URL Category

For a URL category, the web reporting feature can generate data to be included in a category report. For example, for the category 'Sports', the report may contain:

• A list of the top domains that were in the 'Sports' category
• A list of the top users who accessed the 'Sports' category

In all of these examples, these reports are intended to give a comprehensive view about a particular item on the network so that the administrator can take action.

General

For a detailed description on logging pages versus reporting pages, see the Logging Versus Reporting.

Note You can retrieve all the domain information that a user goes to, not necessarily the specific URL that is accessed. For information on a specific URL that the user is accessing, what time they went to that URL, whether that URL is allowed, etc., use the Searching for Transactions Processed by Web Proxy Services , on page 66 on the Web Tracking page.

Note The Web Security appliance only stores data if local reporting is used. If centralized reporting is enabled for the Web Security appliance then the Web Security appliance retains ONLY System Capacity and System Status data. If Centralized Web Reporting is not enabled, the only reports that are generated are System Status and System Capacity.

There are multiple ways to view web reporting data on the Security Management appliance.

• To view interactive report pages, see Web Reporting Page Descriptions, on page 6.
• To generate a report on demand, see Generating Web Reports on Demand , on page 61.
• To schedule generation of reports on a regular, recurring basis, see About Scheduled and On-Demand Web Reports, on page 57.
• To view archived versions of previously run reports (both scheduled and generated on demand), see Viewing and Managing Archived Web Reports, on page 62.
• To view information about individual transactions, see Web Tracking , on page 66.

Setting Up Centralized Web Reporting and Tracking

To set up centralized web reporting and tracking, complete the following steps in order:

Enabling Centralized Web Reporting on the Security Management Appliance

Step 1 Before enabling centralized web reporting, ensure that sufficient disk space is allocated to that service. See Managing Disk Space.

Step 2 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 3 Choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.

Step 4 If you are enabling centralized reporting for the first time after running the System Setup Wizard:

a) Click **Enable**.

b) Review the end user license agreement, then click **Accept**.

Step 5 If you are enabling centralized reporting after it has previously been disabled:

a) Click **Edit Settings**.

b) Select the **Enable Centralized Web Report Services** checkbox.

c) You can address Anonymizing User Names in Web Reports , on page 4 now or later.

Step 6 Submit and commit your changes.

Enabling Centralized Web Reporting on Web Security Appliances

All Web Security appliances should be configured and working as expected before you enable centralized reporting.

You must enable centralized reporting on each Web Security appliance that will use centralized reporting.

See the "Enabling Centralized Reporting" section in AsyncOS for Cisco Web Security Appliances User Guide.

Adding the Centralized Web Reporting Service to Each Managed Web Security Appliance

The steps you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3   If you have already added the Web Security appliance to the list:

a)   Click the name of a Web Security Appliance.

b)   Select the **Centralized Reporting** service.

Step 4   If you have not yet added Web Security appliances:

a)   Click Add Web Appliance.

b)   In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Web Security appliance.

> **Note**   A DNS name may be entered in the IP Address text field, however, it will be immediately resolved to an IP address when you click **Submit**.

c)   The Centralized Reporting service is pre-selected.

d)   Click **Establish Connection.**

e)   Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.

> **Note**   You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

f)   Wait for the Success message to appear above the table on the page.

g)   Click **Test Connection**.

h)   Read test results above the table.

Step 5   Click **Submit**.

Step 6   Repeat this procedure for each Web Security Appliance for which you want to enable Centralized Reporting.

Step 7   Commit your changes.

Anonymizing User Names in Web Reports

By default, user names appear on reporting pages and PDFs. However, to protect user privacy, you may want to make user names unrecognizable in web reports.

✎

> **Note**   Users with Administrator privileges on this appliance can always see user names when viewing interactive reports.

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.

Step 3   Click **Edit Settings**.

Step 4   Select the **Anonymize usernames in reports** checkbox.

Step 5 Submit and commit your change.

Working with Web Security Reports

Web reporting pages allow you to monitor information on one or all of the managed Web Security appliances in your system.

To	See
View options for accessing and viewing report data	Ways to View Reporting Data
Customize your view of the interactive report pages	Customizing Your View of Report Data
Find information about specific transactions within your data	Web Tracking , on page 66
Print or export report information	Exporting Reporting and Tracking Data
Understand the various interactive report pages	Web Reporting Page Descriptions, on page 6
Generate a report on demand	Understanding the Web Reporting Pages on the New Web Interface, on page 33
Schedule reports to run automatically at intervals and times that you specify	About Scheduled and On-Demand Web Reports, on page 57
View archived on-demand and scheduled reports	Viewing and Managing Archived Web Reports, on page 62
Understand how data is gathered	How the Security Management Appliance Gathers Data for Reports

Working with Web Security Reports on the New Web Interface

Web reporting pages allow you to monitor information on one or all of the managed Web Security appliances in your system.

To	See
View options for accessing and viewing report data	Ways to View Reporting Data
Customize your view of the interactive report pages	Customizing Your View of Report Data
Find information about specific transactions within your data	Web Tracking on the New Web Interface, on page 71
Print or export report information	Exporting Reporting and Tracking Data

To	See
Understand the various interactive report pages	Understanding the Web Reporting Pages on the New Web Interface, on page 33

Web Reporting Page Descriptions

> **Note** For information on which of the options on the Web Reporting tab are available as on-demand or scheduled reports, see the About Scheduled and On-Demand Web Reports, on page 57.

Table 1: Web Reporting Tab Details

Web Reporting Menu	Action
Web Reporting Overview , on page 9	The Overview page provides a synopsis of the activity on your Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the Web Reporting Overview , on page 9.
Users Report (Web) , on page 10	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 **Web > Reporting > 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 Report (Web) , on page 10. For information on a specific user in your system, see the User Details (Web Reporting) , on page 11
User Count Report (Web)	The User Count page provides the aggregated information about the total number of authenticated and unauthenticated users of the Web Security appliances with Centralized Reporting enabled. The page lists the unique user count for the last 30 days, 90 days, and 180 days.
	Note System hourly computes the total user count of authenticted and unauthenticated users.

Web Reporting Menu	Action
Web Sites Report , on page 13	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 Report , on page 13.
URL Categories Report , on page 14	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 Report , on page 14.
Application Visibility Report , on page 16	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 Web Security appliance. For more information, see the Application Visibility Report , on page 16.
Anti-Malware Report , on page 18	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 Report , on page 18.
Advanced Malware Protection (File Reputation and File Analysis) Reports , on page 20	There are three reporting pages showing file reputation and analysis data. For more information, see the Advanced Malware Protection (File Reputation and File Analysis) Reports , on page 20.
Client Malware Risk Report , on page 25	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 Risk Report , on page 25.
Web Reputation Filters Report , on page 26	Allows you to view reporting on Web Reputation filtering for transactions during a specified time range. For more information, see the Web Reputation Filters Report , on page 26.
L4 Traffic Monitor Report , on page 27	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 L4 Traffic Monitor Report , on page 27.
SOCKS Proxy Report , on page 29	Allows you to view data for SOCKS proxy transactions, including destinations and users. For more information, see the SOCKS Proxy Report , on page 29.

Web Reporting Menu	Action
Reports by User Location , on page 29	The Reports by User Location page allows you to find out what activities that your mobile users are conducting from their local or remote systems. For more information, see the Reports by User Location , on page 29.
Web Tracking , on page 66	The Web Tracking page allows you to search for the following types of information: • Searching for Transactions Processed by Web Proxy Services , on page 66 allows you to track and see basic web-related information such as the type of web traffic that is being handled by the appliances. This includes information such as time ranges, and UserID and Client IP addresses, but also includes information like certain types of URLs, how much bandwidth that each connection is taking up, or tracking a specific user's web usage. • Searching for Transactions Processed by the L4 Traffic Monitor , on page 70 allows you to search your L4TM data for sites, ports, and client IP addresses involved in malware transfer activity. • Searching for Transactions Processed by the SOCKS Proxy , on page 70 allows you to search for transactions processed by the SOCKS proxy. For more information, see the Web Tracking , on page 66.
System Capacity Page, on page 30	Allows you to view the overall workload that is sending reporting data to the Security Management appliance. For more information, see the System Capacity Page, on page 30.
Data Availability Page, on page 32	Allows you to get a glimpse of the impact of the reporting data on the Security Management appliance for each appliance. For more information, see the Data Availability Page, on page 32.
Scheduled Reports	Allows you to schedule reports for a specified time range. For more information, see the About Scheduled and On-Demand Web Reports, on page 57.
Archived Reports	Allows you to archive reports for a specified time range. For more information, see the Viewing and Managing Archived Web Reports, on page 62.

Note   You can schedule reports for most of the web reporting categories, including additional reports for Extended Top URL Categories and Top Application Types. For more information on scheduling reports, see the About Scheduled and On-Demand Web Reports, on page 57.

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.

Web Reporting Overview

The **Web > Reporting > Overview** page provides a synopsis of the activity on your Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions.

At a high level the **Overview** 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** 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 2: Details on the Web Reporting Overview Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
View Data for	Choose a Web Security appliance for which you want to view Overview data, or choose All Web Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group.
Total Web Proxy Activity	This section allows you to view the web proxy activity that is being reported by the Web Security appliances that are currently managed by the Security Management appliance. This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).
Web Proxy Summary	This section allows you to view the percentage of web proxy activity that are suspect, or clean proxy activity, including the total number of transactions.
L4 Traffic Monitor Summary	This section reports any L4 traffic that is being reported by the Web Security appliances that are currently managed by the Security Management appliance.

Section	Description
Suspect Transactions	This section allows you to view the web transactions that have been labeled as suspect by the administrator.
	This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).
Suspect Transactions Summary	This section allows you to 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.
Top URL Categories by Total Transactions	This section displays the top 10 URL categories that are being blocked, including the type of URL category (vertical scale) and the actual number of times the specific type of category has been blocked (horizontal scale).
	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 15.
Top Application Types by Total Transactions	This section displays the top application types that are being blocked, including the name of the actual application type (vertical scale) and the number of times the specific application has been blocked (horizontal scale).
Top Malware Categories Detected	This section displays all Malware categories that have been detected.
Top Users Blocked or Warned Transactions	This section displays the actual users that are generating the blocked or warned transactions. Users can be displayed by IP address or by user name. To make user names unrecognizable, see Anonymizing User Names in Web Reports , on page 4.
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.

Users Report (Web)

The **Web > Reporting > Users** page provides several links that allow you to view web reporting 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 view the following information pertaining to the users on your system:

Table 3: Details on the Web Reporting Users Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Users by Transactions Blocked	This section lists the top users, by either IP address or user name (vertical scale), and the number of transactions that have been blocked specific to that user (horizontal scale). 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 section Enabling Centralized Web Reporting on the Security Management Appliance , on page 3. The default setting is that all user names appear. To hide user names, see Anonymizing User Names in Web Reports , on page 4.
Top Users by Bandwidth Used	This sections displays the top users, by either IP address or user name (vertical scale), that are using the most bandwidth on the system (horizontal scale represented in gigabyte usage).
Users Table	You can find a specific User ID or Client IP address. In the text field at the bottom of the User section, enter the specific User ID or Client IP address and click on **Find User ID or Client IP Address**. The IP address does not need to be an exact match to return results. From the Users table you can click on a specific user to find more specific information. This information appears on the User Details page. For more information on the User Details page, see the User Details (Web Reporting) , on page 11

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. For information, see Creating the LDAP Server Profile in chapter Integrating With LDAP.

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

To view an example of how the **Users** page may be used, see Example 1: Investigating a User.

Note   You can generate or schedule a report for the Users page. For information, see the About Scheduled and On-Demand Web Reports, on page 57.

User Details (Web Reporting)

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

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

Table 4: Details on the Web Reporting User Details Page

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
URL Categories by Total Transactions	This section lists the specific URL Categories that a specific user is using. 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 15.
Trend by Total Transactions	This graph displays at what times the user accessed the web. 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 section shows matched categories for both completed and blocked transactions. From this section you can also find a specific URL Category. In the text field at the bottom of the section enter the URL Category 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 15.
Domains Matched	From this section you can find out about a specific Domain or IP address that this user has accessed. You can also see the time spent on those categories, and various other information that you have set from the column view. In the text field at the bottom of the section enter the Domain or IP address and click **Find Domain or IP**. The domain or IP address does not need to be an exact match.
Applications Matched	From this section you can find a specific application 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. In the text field at the bottom of the section enter the application name and click **Find Application**. The name of the application does not need to be an exact match.
Malware Threats Detected	From this table you can see the top Malware threats that a specific user is triggering. You can search for data on a specific malware threat name in the Find Malware Threat field. Enter the Malware Threat name and click Find Malware Threat. The name of the Malware Threat does not need to be an exact match.
Policies Matched	From this section you can find the policy groups that applied to this user when accessing the web. In the text field at the bottom of the section enter the policy name 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.

To view an example of how the User Details page may be used, see Example 1: Investigating a User.

User Count Report (Web)

The **Web** >**Reporting** > **User Count** page displays the aggregated information about the total number of authenticated and unauthenticated users of the Web Security appliances with Centralized Reporting enabled. The page lists the unique user count for the last 30 days, 90 days, and 180 days.

Note   System hourly computes the total user count of authenticted and unauthenticated users.

Web Sites Report

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

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

Table 5: Details on the Web Reporting Web Sites Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Domains by Total Transactions	This section lists the top domains that are being visited on the site in a graph format.
Top Domains by Transactions Blocked	This section lists the top domains that triggered a block action to occur per transaction in a graph format. 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.

Section	Description
Domains Matched	This section lists the domains that are that are being visited on the site in an interactive table. From this table you can access more granular information about a specific domain by clicking on the specific domain. 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.
	To view an example of how Web Tracking may be used, see Example 2: Tracking a URL.
	Note If you export this data to a .csv file, only the first 300,000 entries are exported.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

Note You can generate or schedule a report for information on the Web Sites page. For information, see the About Scheduled and On-Demand Web Reports, on page 57.

URL Categories Report

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

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

Table 6: Details on the Web Reporting 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.
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	This section lists the top URL that triggered a block or warning action to occur per transaction in a graph 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.
URL Categories Matched	The URL Categories Matched section 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 15.
URL Filtering Bypassed	Represents policy, port, and admin user agent blocking that occurs before URL filtering.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

Note To generate a more detailed report than this page can provide, see Top URL Categories—Extended, on page 60.

- If Data Availability is used within a scheduled report for URL Categories, and there are gaps in data for any of the appliances, the following message is displayed at the bottom of the page: " Some data in this time range was unavailable." If there are no gaps present, nothing appears.

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 Web Security Appliances User Guide.

- For sites that you feel should be included in existing or other categories, see Reporting Misclassified and Uncategorized URLs , on page 16.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated on your Security Management appliance, as described in Preparing For and Managing URL Category Set Updates.

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

If there is overlap between the contents of old and new categories, you may need to examine report results more carefully to obtain valid statistics. For example, if the "Instant Messaging" and "Web-based Chat" categories have been merged into a single "Chat and Instant Messaging" category during the time frame that you are looking at, visits before the merge to sites covered by the "Instant Messaging" and "Web-based Chat" categories are not counted in the total for "Chat and Instant Messaging". Likewise, visits to instant messaging or Web-based chat sites after the merge would not be included in the totals for the "Instant Messaging" or "Web-based Chat" categories.

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 37 and the Users Page, on page 44 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 42 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 44, 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 66 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.

To view another example of how the URL Categories page may be used, see Example 3: Investigating Top URL Categories Visited.

Reporting Misclassified and Uncategorized URLs

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

https://securityhub.cisco.com/web/submit_urls

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.

Application Visibility Report

✎

Note   For detailed information on Application Visibility, see the 'Understanding Application Visibility and Control' chapter in AsyncOS for Cisco Web Security Appliances User Guide.

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

Not only does application control gives you more granular control over web traffic than just URL filtering, for example, it gives you 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.
- **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.

Note For detailed information on understanding how you can use Application Visibility and Control (AVC) engine to control Facebook activity, see the 'Understanding Application Visibility and Control' chapter in AsyncOS for Cisco Web Security Appliances User Guide.

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

Table 7: Details on the Web Reporting Application Visibility Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Application Types by Total Transactions	This section lists the top application types that are being visited on the site in a graph format. For example, instant messaging tools such as Yahoo Instant Messenger, Facebook, and Presentation application types.
Top Applications by Blocked Transactions	This section lists the top application types that triggered a block action to occur per transaction in a graph format. 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 section shows all the application during a specified time range. This is an interactive table with interactive column headings that you can use to sort data as you need. You can configure the columns that you want to appear in the Applications Matched section. For information on configuring columns for this section, see the Working with Web Security Reports, on page 5. After you have selected the specific items to appear in the Applications table, you can select how many items you want to be displayed from the **Items Displayed** drop-down menu. Choices are: 10, 20, 50, or 100. 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**.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

> **Note** You can generate a scheduled report for information on the Application Visibility page. For information on scheduling a report, see the About Scheduled and On-Demand Web Reports, on page 57.

Anti-Malware Report

The **Web > Reporting > Anti-Malware** 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).

Use this page to help identify and monitor web-based malware threats.

> **Note** To view data for malware found by L4 Traffic Monitoring, see L4 Traffic Monitor Report , on page 27.

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

Table 8: Details on the Web Reporting Anti-Malware Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Malware Categories: Monitored or Blocked	This section displays the top malware categories that are detected by a given category type. This information is displayed in graph format. See Malware Category Descriptions, on page 19 for more information on valid Malware categories.
Top Malware Threats: Monitored or Blocked	This section displays the top malware threats. This information is displayed in graph format.
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 19 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.

> **Tip** To customize your view of this report, see Working with Web Security Reports, on page 5.

Malware Category Report

The Malware Category Report page allows you to view detailed information on an individual Malware Category and what it is doing on your network.

To access the Malware Category report page, perform the following:

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

Step 2 Choose **Monitoring > Anti-Malware** page.

Step 3 In the Malware Categories interactive table, click on a category in the Malware Category column.

Step 4 To customize your view of this report, see Working with Web Security Reports, on page 5.

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 Web Security 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.

Malware Type	Description
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.
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 passphrases 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.

Advanced Malware Protection (File Reputation and File Analysis) Reports

Requirements for File Analysis Report Details

(Cloud File Analysis) Ensure That the Management Appliance Can Reach the File Analysis Server

In order to obtain File Analysis report details, the appliance must be able to connect to the File Analysis server over port 443. See details in Firewall Information.

If your Cisco Content Security Management appliance does not have a direct connection to the internet, configure a proxy server for this traffic (See Upgrade and Update Settings.) If you have already configured the appliance to use a proxy to obtain upgrades and service updates, the existing settings are used.

If you use an HTTPS proxy, the proxy must not decrypt the traffic; use a pass-through mechanism for communications with the File Analysis server. The proxy server must trust the certificate from the Fire Analysis server, but need not provide its own certificate to the File Analysis server.

(Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results

In order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization, you need to join all appliances to the same appliance group.

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Select **Management Appliance > Centralized Services > Security Appliances**.

Step 3 Scroll to the File Analysis section.

Step 4 If your managed appliances are pointed at different File Analysis cloud servers, select the server from which to display result details.

Result details will not be available for files processed by any other cloud server.

Step 5 Enter the Analysis Group ID.

- If you enter the Group ID incorrectly or need to change it for any other reason, you must open a case with Cisco TAC.

- This change takes effect immediately; it does not require a Commit.

- It is suggested to use your CCOID for this value.

- This value is case-sensitive.

- This value must be identical on all appliances that will share data about files that are uploaded for analysis.

- An appliance can belong to only one group.

- You can add a machine to a group at any time, but you can do it only once.

Step 6   Click **Group Now**.

Step 7   Configure the same group on each Web Security appliance that will share data with this appliance.

What to do next

Related Topics

(On-Premises File Analysis) Activate the File Analysis Account

If you have deployed an on-premises (private cloud) Cisco AMP Threat Grid Appliance, you must activate the File Analysis account for your Cisco Content Security Management appliance in order to view report details available on the Threat Grid appliance. You generally only need to do this once.

Before you begin

Ensure that you are receiving System alerts at Critical level.

Step 1   The first time you attempt to access File Analysis report details from the Threat Grid appliance, wait a few minutes and you will receive an alert that includes a link.

If you do not receive this alert, click on the ⚙ icon to load the legacy web interface and choose **Management Appliance > System Administration > Alerts** and click **View Top Alerts**.

Step 2   Click the link in the alert message.

Step 3   If necessary, sign in to your Cisco AMP Threat Grid Appliance.

Step 4   Activate your management appliance account.

Additional Requirements

For any additional requirements, see the Release Notes for your Security Management appliance release, available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format). To identify the filenames associated with a malware instance in your organization, select Advanced Malware Protection report page and click an SHA-256 link in the table. The details page shows associated filenames.

Advanced Malware Protection (File Reputation and File Analysis) Report Pages

Report	Description
Advanced Malware Protection	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.
	Clicking the link at the bottom of Malware Threat File Details report page displays all 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.
	For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection 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.
	The **Malware Files by Category** section shows the percentage of blocked listed file SHAs received from the AMP for Endpoints console that are categorised as **Custom Detection**
	The threat name of a blocked listed file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Malware Threat Files section of the report.
	To view the file trajectory details of a blocked listed file SHA in the AMP for Endpoints console, perform the following steps:
	1. Choose **Reporting** > **Advanced Malware Protection**.
	2. Click on the file SHA link for which you want to view the trajectory details.
	3. Click on the AMP Console link in the **More Details** section.
File Analysis	Displays the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.
	To view more than 1000 File Analysis results, export the data as a .csv file.
	For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are included in the allowed list on the Cisco AMP Threat Grid appliance show as "clean." For information about allowed list, see the AMP Threat Grid 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 Threat Grid link at the bottom of the file analysis details page.
	To view details on the server that analyzed a file, see Requirements for File Analysis Report Details , on page 21.
	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.

Report	Description
AMP Verdict Updates	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 Web Security appliance.
	To view more than 1000 verdict updates, export the data as a .csv file.
	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 Web Security appliances have different verdict updates for the same file, the result with the latest time stamp is displayed.
	Clicking an SHA-256 link displays 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.
	To view all affected transactions for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report), click the link at the bottom of the Malware Threat Files page.

Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A "Blocked by Advanced Malware Protection" column may be hidden by default in applicable reports. To display additional columns, click the Columns link below the table.

For Which Files Are Detailed File Analysis Results Visible in the Cloud?

If you have deployed public-cloud File Analysis, you can view detailed results for all files uploaded from any managed appliance that has been added to the appliance group for File Analysis.

If you have added your management appliance to the group, you can view the list of managed appliances in the group by clicking the button on the **Management Appliance > Centralized Services > Security Appliances**page.

Appliances in the analysis group are identified by the File Analysis Client ID. To determine this identifier for a particular appliance, look in the following location:

Appliance	Location of File Analysis Client ID
Email Security appliance	Advanced Settings for File Analysis section on the **Security Services > File Reputation and Analysis** page.
Web Security appliance	Advanced Settings for File Analysis section on the **Security Services > Anti-Malware and Reputation**page.
Cisco Content Security Management appliance	At the bottom of the **Management Appliance > Centralized Services > Security Appliances** page.

Related Topics

Client Malware Risk Report

The **Web > Reporting > Client Malware Risk** page is a security-related reporting page that can be used to monitor client malware risk activity.

From the Client Malware Risk page, a system administrator can see which of their users are encountering the most blocks or warnings. Given the information gathered from this page, the administrator can click on the user link to view what this user doing on the web that makes them run into so many blocks or warnings and setting off more detections than the rest of the users on the network.

Additionally, the Client Malware Risk page lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM). A computer that connects frequently to malware sites may be infected with malware that is trying to connect to a central command and control server and should be disinfected.

The following table describes the information on the Client Malware Risk page.

Table 9: Client Malware Risk Report Page Components

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report. For more information, see Choosing a Time Range for Reports.
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 ten computers in your organization that most frequently connect to malware sites.
	This chart is the same as the "Top Client IPs" chart on the L4 Traffic Monitor Report , on page 27. See that section for more information and chart options.
Web Proxy: Client Malware Risk	The Web Proxy: Client Malware Risk table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section.
	You can click each user in this table to view the User Details page associated with that client. For information about that page, see the User Details (Web Reporting) , on page 11.
	Clicking on any of the links in the table allows you to view more granular details about individual users and what activity they are performing that is triggering the malware risk. For example, clicking on the link in the "User ID / Client IP Address" column takes you to a User page for that user.
L4 Traffic Monitor: Clients by Malware Risk	This table displays IP addresses of computers in your organization that frequently connect to malware sites.
	This table is the same as the "Client Source IPs" table on the L4 Traffic Monitor Report , on page 27. For information about working with this table, see that section.

🔍

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

Web Reputation Filters Report

The **Web > Reporting > Web Reputation Filters** allows you to view the results of your set Web Reputation filters for transactions during a specified time range.

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 Web Security 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 IronPort AsyncOS for Web User Guide.

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

Table 10: Details on the Web Reporting Web Reputation Filters Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.

Section	Description
Web Reputation Actions (Trend)	This section, in graph format, displays the total number of web reputation actions (vertical) against the time specified (horizontal timeline). From this you can see potential trends over time for web reputation actions.
Web Reputation Actions (Volume)	This section displays the web reputation action volume in percentages by transactions.
Web Reputation Threat Types Blocked by WBRS	This section displays the types of threats found in transactions that were blocked by Web Reputation filtering. Note: WBRS cannot always identify the threat type.
Threat Types Detected in Other Transactions	This section displays the type of threats found in transactions that were not blocked by Web Reputation filtering. 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.

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

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 AsyncOS for Cisco Web Security Appliances User Guide.

L4 Traffic Monitor Report

The **Web > Reporting > L4 Traffic Monitor** page displays information about malware ports and malware sites that the L4 Traffic Monitors on your Web Security appliances have 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 each Web Security 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.)

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

Table 11: L4 Traffic Monitor Report Page Components

Section	Description
Time Range (drop-down list)	A menu that allows you to choose a time range on which to report. For more information, see Choosing a Time Range for Reports.
Top Client IPs	This section displays, in graph format, the IP addresses of computers in your organization that most frequently connect to malware sites.
	Click the Chart Options link below the chart to change the display from total Malware Connections Detected to Malware Connections Monitored or Malware Connections Blocked.
	This chart is the same as the "L4 Traffic Monitor: Malware Connections Detected" chart on the Client Malware Risk Report , on page 25.
Top Malware Sites	This section displays, in graph format, the top malware domains detected by the L4 Traffic Monitor.
	Click the Chart Options link below the chart to change the display from total Malware Connections Detected to Malware Connections Monitored or Malware Connections Blocked.
Client Source IPs	This table displays 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 Port. 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 L4 Traffic Monitor tab on the Web > Reporting > Web Tracking page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 70.
	This table is the same as the "L4 Traffic Monitor - Clients by Malware Risk" table on the Client Malware Risk Report , on page 25.
Malware Ports	This table displays the ports on which the L4 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 L4 Traffic Monitor tab on the Web > Reporting > Web Tracking page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 70.

Section	Description
Malware Sites Detected	This table displays the domains on which the L4 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 L4 Traffic Monitor tab on the Web > Reporting > Web Tracking page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 70.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

Related Topics

- Troubleshooting L4 Traffic Monitor Reports , on page 80

SOCKS Proxy Report

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

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 AsyncOS for Cisco Web Security Appliances User Guide.

Related Topics

- Searching for Transactions Processed by the SOCKS Proxy , on page 70

Reports by User Location

The **Web > Reporting > Reports by User Location** Page allows you to find out what activities your mobile users are conducting from their local or remote systems.

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.

From the **Reports by User Location** page, you can view the following information:

Table 12: Details on the Web Reporting Reports by User Location Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Total Web Proxy Activity: Remote Users	This section displays, in graph format, the activity of your remote users (vertical) over the specified time (horizontal).
Web Proxy Summary	This section displays a summary of the activities of the local and remote users on your system.
Total Web Proxy Activity: Local Users	This section displays, in graph format, the activity of your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Detected: Remote Users	This section displays, in graph format, the suspect transactions that have been detected due to access policies that you have defined for your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	This section displays a summary of suspected transactions of the remote users on your system.
Suspect Transactions Detected: Local Users	This section displays, in graph format, the suspect transactions that have been detected due to access policies that you have defined for your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	This section displays a summary of suspected transactions of the local users on your system.

From the **Reports by User Location** page you can generate reports showing the activity of local and remote users. This allows you to easily compare local and remote activities of your users.

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

Note   You can generate a scheduled report for information on the Reports by User Location page. For information on scheduling a report, see the About Scheduled and On-Demand Web Reports, on page 57.

System Capacity Page

The **Web > Reporting > System Capacity** page allows you to view the overall workload that is put on the Security Management appliance by the Web Security appliances. Most importantly, you can use the System Capacity page to track growth over time and plan for system capacity. Monitoring your Web Security appliances

ensures that the capacity is appropriate to your volumes. Over time, volume inevitably rises and appropriate monitoring ensures that additional capacity or configuration changes can be applied proactively.

The System Capacity page can be used to determine the following information:

- Identify when Web Security appliances are exceeding recommended CPU capacity; this enables you to determine when configuration optimization or additional appliances are needed.
- For troubleshooting, identify which parts of the system are using the most resources.
- Identify response time and Proxy buffer memory.
- Identify the transactions per second, and any connections that are outstanding.

Viewing the System Capacity Report

Step 1   On the Security Management appliance, choose **Web > Reporting > System Capacity**.

Step 2   To view different types of data, click **Columns** and choose the data to view.

Step 3   To see the system capacity for a single appliance, click the appliance in the Web Security appliance column in the Overview of Averaged Usage and Performance table.

The System Capacity graphs appear for that appliance. The graphs on the page are divided into two sets:

How to Interpret the Data You See on the System Capacity Page

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

- Day Report— The Day report queries the hour table and displays the exact number of queries that have been received by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table.
- Month Report— The Month report queries the day tables for the 30 or 31 days (dependent on the number of days in the month), giving you an exact report on the number of queries over 30 or 31 days. Again, this is an exact number.

The 'Maximum' value indicator on the System Capacity page is the highest value seen for the specified period. The 'Average' value is the average of all values for the specified period. The period of aggregation depends on the interval selected for that report. For example, you can choose to see the Average and Maximum values for each day if the chart is for a month period.

Note   If you select **Year** for the time range for other reports, we recommend that you select the largest time range, 90 days.

System Capacity - System Load

The first four graphs on the System Capacity window show the system load reports. These reports show the overall CPU usage on the appliances. AsyncOS is optimized to use idle CPU resources to improve transaction

throughput. High CPU usage may not indicate a system capacity problem. If the high CPU usage is coupled with consistent, high-volume memory page swapping, you may have a capacity problem. This page also shows a graph that displays the amount of CPU used by different functions, including processing for the Web Security appliance reporting. The CPU-by-function graph is an indicator of which areas of the product use the most resources on your system. If you need to optimize your appliance, this graph can help you determine which functions may need to be tuned or disabled.

Additionally, the Response Time/Latency and Transactions Per Second graphs shows the overall response time (in milliseconds), and transactions per second for the date range specified in the Time Range drop-down menu.

System Capacity - Network Load

The next graphs on the System Capacity window show the outgoing connections, the bandwidth out, and the proxy buffer memory statistics. You can view the results for a day, week, month, or year. It is important to understand the trends of normal volume and spikes in your environment.

The Proxy Buffer Memory may indicate spikes in network traffic during normal operation, but if the graph climbs steadily to the maximum, the appliance may be reaching its maximum capacity and you should consider adding capacity.

These charts are on the same page as the charts described in System Capacity - System Load , on page 31, below those charts.

Note About Proxy Buffer Memory Swapping

The system is designed to swap proxy buffer memory regularly, so some proxy buffer memory swapping is expected and is not an indication of problems with your appliance. Unless the system *consistently* swaps proxy buffer memory in high volumes, proxy buffer memory swapping is normal and expected behavior. If your system runs with extremely high volumes, and consistently swaps proxy buffer memory due to the high volumes, you may need to add Web Security appliances to your network or tune your configuration to ensure maximum throughput to improve performance.

Data Availability Page

The **Web > Reporting > Data Availability** page provides an overview of the date ranges for which reporting and web tracking data are available on the Security Management appliance for each managed Web Security appliance.

Note If Web Reporting is disabled, the Security Management appliance will not pull any new data from the Web Security appliance, but previously retrieved data is still present on the Security Management appliance.

If the status is different between The Web Reporting 'From' and 'To' columns, and the Web Reporting and Tracking 'From' and 'To' columns, the most severe consequence appears in the Status column.

For information about purging of data, see the Managing Disk Space.

Note   If Data Availability is used within a scheduled report for URL Categories, and there are gaps in data for any of the appliances, the following message is displayed at the bottom of the page: "Some data in this time range was unavailable." If there are no gaps present, nothing appears.

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 Web Security appliances under the **Reports** drop-down of the web interface. For more information, see Using the Interactive Report Pages. If your Web Security appliances are running earlier releases of AsyncOS, not all of these reports are available.

Table 13: 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 Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the Overview Page, on page 35.
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 Web Security appliance. For more information, see the Application Visibility Page, on page 37.
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 39.
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 41.

Reports Drop-down Option	Action
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 42.
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 44. For information on a specific user in your system, see the User Details Page (Web Reporting) , on page 45.
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 47.
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 48.
Threat Reports	

Reports Drop-down Option	Action
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 49.
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 Risk Report , on page 54.
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 55.

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 Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions.

To view the Overview report page, select **Web** from the Product drop-down and choose **Monitoring > Overview** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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 14: 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.
View Data for (drop-down list)	Choose a Web Security appliance for which you want to view Overview data, or choose All Web Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group
Total Web Proxy Activity	You can view the web proxy activity that is being reported by the Web Security 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 Web Security 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 15.

Section	Description
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.
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. To make user names unrecognizable, see Anonymizing User Names in Web Reports , on page 4.

Application Visibility Page

✎

Note   For detailed information on Application Visibility, see the 'Understanding Application Visibility and Control' chapter in User Guide for AsyncOS for Cisco Web Security Appliances.

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

To view the Application Visibility report page, select **Web** from the product drop-down and choose **Monitoring > Application Visibility** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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.

- **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.

Note For detailed information on understanding how you can use Application Visibility and Control (AVC) engine to control Facebook activity, see the 'Understanding Application Visibility and Control' chapter in User Guide for AsyncOS for Cisco Web Security Appliances.

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

Table 15: 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.
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.
	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.
	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.

Note   To customize your view of this report, see Working with Web Security Reports, on page 5.

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 Web Security 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, select **Web** from the Product drop-down and choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

The Layer 4 Traffic Monitor listens to network traffic that comes in over all ports on each Web Security 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 16: 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.
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 (Web Reports Only) Choosing Which Data to Chart. This chart is the same as the "Layer 4 Traffic Monitor: Malware Connections Detected" chart on the Client Malware Risk Report , on page 54.
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 (Web Reports Only) Choosing Which Data to Chart.

Section	Description
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 L4 Traffic Monitor , on page 70.
	This chart is the same as the "Layer 4 Traffic Monitor: Malware Connections Detected" chart on the Client Malware Risk Report , on page 54.
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 L4 Traffic Monitor , on page 70.
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 L4 Traffic Monitor , on page 70.

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

Related Topics

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, select **Web** from the product drop-down and choose **Monitoring > SOCKS Proxy** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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 Web Security Appliances*.

Table 17: 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.
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.
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.
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**.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

Related Topics

Searching for Transactions Processed by the SOCKS Proxy , on page 70

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, select **Web** from the Product drop-down and choose **Monitoring > URL Categories** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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

Table 18: 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.
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.
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.
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.

Section	Description
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 15.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

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 Web Security Appliances User Guide.

- For sites that you feel should be included in existing or other categories, see Reporting Misclassified and Uncategorized URLs , on page 16.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated on your Security Management appliance, as described in Preparing For and Managing URL Category Set Updates.

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

If there is overlap between the contents of old and new categories, you may need to examine report results more carefully to obtain valid statistics. For example, if the "Instant Messaging" and "Web-based Chat" categories have been merged into a single "Chat and Instant Messaging" category during the time frame that you are looking at, visits before the merge to sites covered by the "Instant Messaging" and "Web-based Chat" categories are not counted in the total for "Chat and Instant Messaging". Likewise, visits to instant messaging or Web-based chat sites after the merge would not be included in the totals for the "Instant Messaging" or "Web-based Chat" categories.

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 37 and the Users Page, on page 44 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 42 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 44, 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 66 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.

To view another example of how the URL Categories page may be used, see Example 3: Investigating Top URL Categories Visited.

Reporting Misclassified and Uncategorized URLs

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

https://securityhub.cisco.com/web/submit_urls

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.

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, select **Web** from the Product drop-down and choose **Monitoring > Users** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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 Web Security 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 19: 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.

Section	Description
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 Enabling Centralized Web Reporting on the Security Management Appliance , on page 3. The default setting is that all user names appear. To hide user names, see Anonymizing User Names in Web Reports , on page 4. To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart.
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.
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 45

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.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

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 20: 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.
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 15.
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 15.
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.

Section	Description
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, select **Web** from the Product drop-down and choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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

Table 21: 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.
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.
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. 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. To view an example of how Web Tracking may be used, see Example 2: Tracking a URL.

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

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, select **Web** from the **Product** drop-down and choose **Monitoring > HTTPS Reports** from the **Reports** drop-down. For more information, see Using the Interactive Report Pages.

Table 22: 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 Choosing a Time Range for Reports.
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.

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, select **Web** from the Product drop-down and choose **Monitoring > Anti-Malware** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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 39

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

Table 23: 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.
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 19 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.
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.
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 19 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.

Tip   To customize your view of this report, see Working with Web Security Reports, on page 5.

Malware Category Report

The Malware Category Report page allows you to view detailed information on an individual Malware Category and what it is doing on your network.

To access the Malware Category report page, perform the following:

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

Step 2   Choose **Monitoring > Anti-Malware** page.

Step 3   In the Malware Categories interactive table, click on a category in the Malware Category column.

Step 4   To customize your view of this report, see .

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 Web Security 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.

Malware Type	Description
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.
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 passphrases 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.

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 Web Security Appliances*.

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

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

- Advanced Malware Protection - AMP Summary, on page 53

- Advanced Malware Protection - File Analysis, on page 54

Related Topics

- Requirements for File Analysis Report Details , on page 21

- Identifying Files by SHA-256 Hash , on page 22

- Viewing File Reputation Filtering Data in Other Reports , on page 24

- About Web Tracking and Advanced Malware Protection Features , on page 77

Advanced Malware Protection - AMP Summary

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 Web Security 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 Web Security 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

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 Threat Grid Appliance: Files that are included in the allowed list on the Cisco AMP Threat Grid appliance show as "clean." For information about allowed list, see the AMP Threat Grid 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 Threat Grid link at the bottom of the file analysis details page.

To view details on the server that analyzed a file, see Requirements for File Analysis Report Details , on page 21.

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.

Client Malware Risk Report

The **Client Malware Risk** report page is a security-related reporting page that can be used to monitor client malware risk activity.

To view the Client Malware Risk report page, select **Web** from the Product drop-down and choose **Monitoring > Client Malware Risk** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

From the Client Malware Risk report page, a system administrator can see which of their users are encountering the most blocks or warnings. Given the information gathered from this page, the administrator can click on the user link to view what this user doing on the web that makes them run into so many blocks or warnings and setting off more detections than the rest of the users on the network.

Additionally, the Client Malware Risk page lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM). A computer that connects frequently to malware sites may be infected with malware that is trying to connect to a central command and control server and should be disinfected.

The following table describes the information on the Client Malware Risk page.

Table 24: Details on Client Malware Risk 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.
Web Proxy: Top Clients Monitored or Blocked	You can view the top ten users that have encountered a malware risk, 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.
L4 Traffic Monitor: Malware Connections Detected	You can view the IP addresses of the ten 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 (Web Reports Only) Choosing Which Data to Chart. This chart is the same as the "Top Client IPs" chart on the Layer 4 Traffic Monitor Page, on page 39.
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. You can click each user in this table to view the User Details page associated with that client. For information about that page, see the User Details Page (Web Reporting) , on page 45. You can click on any of the links in the table to view more granular details about individual users and what activity they are performing that is triggering the malware risk.
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. This table is the same as the "Client Source IPs" table on the Layer 4 Traffic Monitor Page, on page 39.

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

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, select **Web** from the Product drop-down and choose **Monitoring > Web Reputation Filters** from the Reports drop-down. For more information, see Using the Interactive Report Pages.

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 Web Security 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 Web Security Appliances*.

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

Table 25: 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.

Section	Description
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.
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. 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.

🔍

Tip To customize your view of this report, see Working with Web Security Reports, on page 5.

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 Web Security Appliances*.

About Scheduled and On-Demand Web Reports

Except as noted, you can generate the following types of Web Security reports either as scheduled or on-demand reports:

- Web Reporting Overview—For information on what is included on this page, see the Web Reporting Overview , on page 9.
- Users—For information on what is included on this page, see the Users Report (Web) , on page 10.
- Web Sites—For information on what is included on this page, see the Web Sites Report , on page 13.

- URL Categories—For information on what is included on this page, see the URL Categories Report , on page 14.
- Top URL Categories — Extended: For information on how to generate a report for Top URL Categories — Extended, see the Top URL Categories—Extended, on page 60.

This report is not available as an On-Demand report.

- Application Visibility—For information on what is included on this page, see the Application Visibility Report , on page 16.
- Top Application Types — Extended: For information on how to generate a report for Top URL Categories — Extended, see the Top Application Types—Extended, on page 61.

This report is not available as an On-Demand report.

- Anti-Malware—For information on what is included on this page, see the Anti-Malware Report , on page 18.
- Client Malware Risk—For information on what is included on this page, see the Client Malware Risk Report , on page 25.
- Web Reputation Filters—For information on what is included on this page, see the Web Reputation Filters Report , on page 26.
- L4 Traffic Monitor—For information on what is included on this page, see the L4 Traffic Monitor Report , on page 27.
- Mobile Secure Solution—For information on what is included on this page, see the Reports by User Location , on page 29.
- System Capacity—For information on what is included on this page, see the System Capacity Page, on page 30.

Scheduling Web Reports

This section includes the following:

Note You can choose to make user names unrecognizable in all reports. For information, see Anonymizing User Names in Web Reports , on page 4.

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.

Storage of Scheduled Web Reports

The Security Management appliance retains the most recent reports that it generates — up to 30 of the most recent instances of each scheduled report, and up to 1000 total versions for all reports.

Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 30 instances applies to each scheduled report with the same name and time range.

Archived reports are stored in the /periodic_reports directory on the appliance. (See IP Interfaces and Accessing the Appliance for more information.)

Related Topics

- Viewing and Managing Archived Web Reports, on page 62

Adding Scheduled Web Reports

Step 1   On the Security Management appliance, choose **Web > Reporting > Scheduled Reports**.

Step 2   Click **Add Scheduled Report**.

Step 3   From drop-down menu next to **Type**, choose your report type.

Step 4   In the **Title** field, type 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** drop-down menu.

Step 6   Choose 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   From the drop-down list next to **Number of Items**, choose the number of items that you want to be included in the generated report.

Valid values are from 2 through 20. The default value is 5.

Step 8   For **Charts**, click the default chart under **Data to display** and choose the data to display in each chart in the report.

Step 9   From the drop-down list next to **Sort Column**, select the column to sort the data by for this report. This allows you to create a scheduled report of Top 'N' items by any column available in the scheduled report.

Step 10   From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

Step 11   In the **Email** text field, type in the email address where the generated report will be sent.

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

Step 12   Click **Submit**.

Editing Scheduled Web Reports

To edit reports, go to the **Web > Reporting > Scheduled Reports** page and select the check boxes corresponding to the reports that you want to edit. Modify settings then click **Submit** to submit your changes on the page, then click the **Commit Changes** button to commit your changes on the appliance.

Deleting Scheduled Web Reports

To delete reports, go to the **Web > Reporting > Scheduled Reports** page and select the check boxes corresponding to the reports that you want to delete. To remove all scheduled reports, select the **All** check box, **Delete** and **Commit** your changes. Note that archived versions of deleted reports are not deleted.

Additional Extended Web Reports

Two additional reports are available only as Scheduled Reports on the Security Management appliance:

Top URL Categories—Extended

The Top URL Categories —Extended report is useful for administrators who want to receive more detailed information than the URL Categories report can provide.

For example, in a typical URL Categories report, you can gather information measuring bandwidth usage by a particular employee at a larger URL Category level. To generate a more detailed report that monitors bandwidth usage for the top ten URLs for each URL Category, or top five users for each URL Category, use the Top URL Categories —Extended report.

> **Note** The maximum number of reports that can be generated using this type of report is 20.

To generate a Top URL Categories—Extended report, perform the following:

Step 1 On the Security Management appliance, choose **Web> Reporting > Scheduled Reports**.

Step 2 Click **Add Scheduled Report**.

Step 3 From the drop-down menu next to Type, choose **Top URL categories — Extended**.

Step 4 In the **Title** text field, type the title of your URL extended report.

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

Step 6 Choose the format for the generated report.

The default format is PDF.

Step 7 From the drop-down list next to **Number of Items**, select the number of URL Categories that you want to be included in the generated report.

Valid values are from 2 through 20. The default value is 5.

Step 8 From the drop-down list next to **Sort Column**, select the column to sort the data by for this report. This allows you to create a scheduled report of Top 'N' items by any column available in the scheduled report.

Step 9 For **Charts**, click the default chart under **Data to display** and choose the data to display in each chart in the report.

Step 10 From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

Step 11 In the **Email** text field, type in the email address where the generated report will be sent.

Step 12   Click **Submit**.

Top Application Types—Extended

To generate a Top Application Type—Extended report, perform the following:

Step 1   On the Security Management appliance, choose **Web> Reporting > Scheduled Reports**.

Step 2   Click **Add Scheduled Report**.

Step 3   From the drop-down menu next to Type, choose **Top Application Types — Extended**.

The options on the page will change.

Step 4   In the **Title** text field, type the title of your report.

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

Step 6   Choose the format for the generated report.

The default format is PDF.

Step 7   From the drop-down list next to **Number of Items**, select the number of Application Types that you want to be included in the generated report.

Valid values are from 2 through 20. The default value is **5**.

Step 8   From the drop-down list next to **Sort Column**, select the type of column that you want to appear in the table. Choices include: Transactions Completed, Transactions Blocked, Transaction Totals.

Step 9   For **Charts**, click a default chart under **Data to display** and choose the data to display in each chart in the report.

Step 10   From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

Step 11   In the **Email** text field, type in the email address where the generated report will be sent.

Step 12   Click **Submit**.

Generating Web Reports on Demand

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

Note   Some reports are available only as Scheduled Reports, not on demand. See Additional Extended Web Reports, on page 60.

To generate a report on demand, perform the following:

Step 1   On the Security Management appliance, choose, **Web > Reporting > Archived Reports**.

Step 2   Click on **Generate Report Now**.

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 Title text field, type 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 Format section, choose the format of the report.

Choices include:

- 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.

- CSV. Create an ASCII text file that contains raw data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.

Step 7   Depending on the options available for the report, choose:

- **Number of rows**: The number of rows of data to display in the table.

- **Charts**: Which data to display in the chart(s) in the report:

- Click the default option under Data to display.

- **Sort Column**: The column to sort by for each table.

Step 8   From the Delivery Option section, choose the following:

- If you want this report to appear on the Archived Reports page, select the **Archive Report** checkbox.

Note   Domain-Based Executive Summary reports cannot be archived.

- Check the **Email now to recipients** checkbox to email the report.

- In the text field, type in the recipient email addresses for the report.

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

Archived Web Reports Page

Viewing and Managing Archived Web Reports

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

Step 1   Go to **Web > Reporting > Archived Reports**.

Step 2   To view a report, click the report names in the Report Title column. The Show drop-down menu filters the types of reports that are listed on the **Archived Reports** page.

Step 3   To locate a particular report if the list is long, filter the list by choosing a report type from the **Show** menu, or click a column heading to sort by that column.

What to do next

Related Topics

Schedule and Archive Web Reports on the New Web Interface

Scheduling Web Reports on the New Web Interface

This section includes the following:

Note   You can choose to make user names unrecognizable in all reports. For information, see Anonymizing User Names in Web Reports , on page 4.

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

Step 1 On the Security Management appliance, choose **Web** from the Product drop-down. For more information, see Using the Interactive Report Pages.

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

Step 3 In the Schduled / Archived tab, click the + button.

Step 4 Select your report type from the **Report Type** drop-down menu.

Step 5 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 6 Choose the time range for the report from the **Time Range to Include** drop-down menu.

Step 7 Choose the format for the generated report.

The default format is PDF.

Step 8 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 9 From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

Step 10 Select the language in which the report must be generated from the **Report Language** drop-down list.

Step 11 Click **Submit**.

Editing Scheduled Web Reports on the New Web Interface

To edit reports on the new web interface of your appliance, select **Web** from the Product drop-down and choose **Monitoring > Scheduled & Archive** page. Click on the link corresponding to the Report Title of reports that you want to edit. Modify settings 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, select **Web** from the Product drop-down and 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

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

Note Some reports are available only as Scheduled Reports, not on demand. See Additional Extended Web Reports, on page 60.

To generate a report on demand, perform the following:

Step 1 On the Security Management appliance, select **Web** from the Product drop-down and 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.

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

Step 2 Choose **Web** from the Product drop-down and 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.

Web Tracking

Use the Web Tracking page to search for 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:

For more information about the distinction between the Web Proxy and the L4 Traffic Monitor, see the "Understanding How the Web Security Appliance Works" section in AsyncOS for Cisco Web Security Appliances User Guide.

Related Topics

Searching for Transactions Processed by Web Proxy Services

Use the **Proxy Services** tab on the **Web > Reporting > Web Tracking** page to search web tracking data aggregated from individual security components and acceptable use enforcement components. This data does not include L4 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 Web Tracking usage, see the Example 1: Investigating a User.

For an example of how the Proxy Services tab can be used with other web reporting pages, see the Using The URL Categories Page in Conjunction with Other Reporting Pages, on page 15.

Step 1 On the Security Management appliance, choose **Web > Reporting > Web Tracking**.

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

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

Step 4 Enter search criteria:

Table 26: 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.
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 . . If the set of URL categories has been updated, some categories may be labeled "Deprecated." Deprecated categories are no longer being used for new transactions. However, you can still search for recent transactions that occurred while the category was active. For more information about URL category set updates, see URL Category Set Updates and Reports , on page 15. All recent transactions that match the category name are included, regardless of the engine name noted in the drop-down list.
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.

Option	Description
Policy	To filter by a policy group, select **Filter by Policy** and enter a policy group name by which to filter. Make sure that you have declared the policy on the Web Security appliance.
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 19.
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.
AnyConnect Secure Mobility	To filter by remote or local access, select **Filter by 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.)
Web Appliance	To filter by a specific Web appliance, click on the radio button next to **Filter by Web Appliance** and enter the Web appliance name in the text field. If you select **Disable Filter**, the search includes all Web Security appliances associated with the Security Management appliance.
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.

Step 5   Click **Search**.

What to do next

Related Topics

Malware Category Descriptions

The Web Security 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.

Malware Type	Description
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 passphrases 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 L4 Traffic Monitor

The L4 Traffic Monitor tab on the **Web > 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
- 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
- The Web Security appliance that processed the connection

The first 1000 matching search results are displayed.

To view the hostname at the questionable site or the Web Security 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 L4 Traffic Monitor Report , on page 27.

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.

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

Related Topics

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:

-

-

-

-

-

For more information about the distinction between the Web Proxy and the Layer4 Traffic Monitor, see the "Understanding How the Web Security Appliance Works" section in *User Guide for AsyncOS for Cisco Web Security 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 Web Tracking usage, see the Example 1: Investigating a User.

For an example of how the Proxy Services tab can be used with other web reporting pages, see the Using The URL Categories Page in Conjunction with Other Reporting Pages, on page 15.

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

Step 2 Choose **Tracking > Proxy Services**.

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

Step 4 Enter search criteria:

Table 27: 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.
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 . . If the set of URL categories has been updated, some categories may be labeled "Deprecated." Deprecated categories are no longer being used for new transactions. However, you can still search for recent transactions that occurred while the category was active. For more information about URL category set updates, see URL Category Set Updates and Reports , on page 15. All recent transactions that match the category name are included, regardless of the engine name noted in the drop-down list.
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.

Option	Description
Policy	To filter by a policy group, select **Filter by Policy** and enter a policy group name by which to filter.
	Make sure that you have declared the policy on the Web Security appliance.
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 19.
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.
AnyConnect Secure Mobility	To filter by remote or local access, select **Filter by 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.)
Web Appliance	To filter by a specific Web appliance, click on the radio button next to **Filter by Web Appliance** and enter the Web appliance name in the text field.
	If you select **Disable Filter**, the search includes all Web Security appliances associated with the Security Management appliance.
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 Web Security 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.

Malware Type	Description
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.
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 passphrases 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.

Malware Type	Description
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

- The Web Security appliance that processed the connection

To view the hostname at the questionable site or the Web Security 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 39.

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.

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

Step 2 Choose **Tracking > SOCKS Proxy**.

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

Step 4 Enter search criteria.

Step 5 Click **Search**.

What to do next

Related Topics

SOCKS Proxy Report , on page 29

Working with Web Tracking Search Results

Displaying More Web Tracking Search Results

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 Web Security 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.

To View	Do This
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 Advanced Malware Protection Features

When searching for file threat information in Web Tracking, keep the following points in mind:

- To search for malicious files found by the file reputation service, select **Known Malicious and High-Risk Files** for the **Filter by Malware Category** option in the Malware Threat area in the Advanced section in Web Tracking.

- Web Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a transaction was processed. For example, if a file was initially found to be clean, then a verdict update found the file to be malicious, only the clean verdict appears in Tracking results.

  "Block - AMP" in search results means the transaction was blocked because of the file's reputation verdict.

  In Tracking details, the "AMP Threat Score" is the best-effort score that the cloud reputation service provides when it cannot determine a clear verdict for the file. In this situation, the score is between 1 and 100. (Ignore the AMP Threat Score if an AMP Verdict is returned or if the score is zero.) The appliance compares this score to the threshold score (configured on the Security Services > Anti-Malware and Reputation page) to determine what action to take. By default, files with scores between 60 and 100 are considered malicious. Cisco does not recommend changing the default threshold score. The WBRS score is the reputation of the site from which the file was downloaded; this score is not related to the file reputation.

- Verdict updates are available only in the AMP Verdict Updates report. The original transaction details in Web Tracking are not updated with verdict changes. To see transactions involving a particular file, click a SHA-256 in the verdict updates report.

- Information about File Analysis, including analysis results and whether or not a file was sent for analysis, are available only in the File Analysis report.

  Additional information about an analyzed file may be available from the cloud. To view any available File Analysis information for a file, select **Reporting > File Analysis** and enter the SHA-256 to search for the file, or click the SHA-256 link in Web Tracking details. If the File Analysis service has analyzed the file from any source, you can see the details. Results are displayed only for files that have been analyzed.

  If the appliance processed a subsequent instance of a file that was sent for analysis, those instances will appear in Web Tracking search results.

Related Topics

- Identifying Files by SHA-256 Hash , on page 22

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.

Troubleshooting Web Reporting and Tracking

See also Troubleshooting All Reports.

Centralized Reporting Is Enabled Properly But Not Working

Problem

You have enabled centralized web reporting as directed, but it is not working.

Solution

If there is no disk space allocated for reporting, centralized web reporting will not work until disk space is allocated. As long as the quota you are setting the Web Reporting and Tracking to is larger than the currently used disk space, you will not lose any Web Reporting and Tracking data. See the Managing Disk Space, for more information.

Advanced Malware Protection Verdict Updates Report Results Differ

Problem

A Web Security appliance and an Email Security appliance sent the same file for analysis, and the AMP Verdict Updates reports for Web and Email show different verdicts for that file.

Solution

This situation is temporary. Results will match once all verdict updates have been downloaded. Allow up to 30 minutes for this to occur.

Issues Viewing File Analysis Report Details

File Analysis Report Details Are Not Available

Problem

File Analysis report details are not available.

Solution

See Requirements for File Analysis Report Details , on page 21.

Error When Viewing File Analysis Report Details

Problem

No cloud server configuration is available, error appears when you attempt to view File Analysis report details.

Solution

Go to **Management Appliance > Centralized Services > Security Appliances** and add at least one Web Security appliance that has the File Analysis feature enabled.

Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance

Problem

You see an API key, registration, or activation error when attempting to view File Analysis report details.

Solution

If you are using a private cloud (on-premises) Cisco AMP Threat Grid appliance for file analysis, see (On-Premises File Analysis) Activate the File Analysis Account , on page 22.

If your Threat Grid appliance hostname changes, you must repeat the process in the referenced procedure.

Expected Data Is Missing from Reporting or Tracking Results

Problem

Expected data is missing from reporting or tracking results.

Solution

Possible causes:

- Make sure you have selected the desired time range.
- For tracking results, be sure you are viewing all matching results. See Displaying More Web Tracking Search Results , on page 76.
- Data transfer between Web Security appliances and the Cisco Content Security Management appliance may have been interrupted, or data may have been purged. See Data Availability Page, on page 32.
- If an upgrade changes the way information is reported or tracked, transactions that occurred before upgrade may not be represented as expected. To see if your release has this type of change, see the Release Notes for your release at the location specified in Documentation.
- For missing results in Web Proxy Services tracking search results, see Searching for Transactions Processed by Web Proxy Services , on page 66.
- For unexpected results when filtering by user requested transactions, see the User Request row of the table in Searching for Transactions Processed by Web Proxy Services , on page 66.

PDF Shows Only a Subset of Web Tracking Data

Problem

PDF shows only some of the data that is visible on the Web Tracking page.

Solution

For information about what data is included in and omitted from PDFs and CSV files, see the web tracking information in the table in Exporting Reporting and Tracking Data.

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 Report , on page 25
- Searching for Transactions Processed by the L4 Traffic Monitor , on page 70

Exported .CSV file is Different From Web Interface Data

Problem

Domains Matched data exported to .csv file differs from the data shown in the Web interface.

Solution

For performance reasons, only the first 300,000 entries are exported as .csv.

Issues Exporting Web Tracking Search Results

Problem

Web tracking search results display an "Out of Memory" errors when you simultaneously run multiple large search queries.

Solution

You can increase the heap size of the memory to 1024 MB or more or reduce the time range of your search criteria as a workaround. Keep in mind that increasing the heap size of the memory can cause memory-related issues.