Product Guide

McAfee Content Security Reporter 2.4.0

Contents

1 Introduction

McAfee® Content Security Reporter is a reporting software solution that helps you identify and analyze a broad range of data collected from your network devices.

Contents

About Content Security Reporter

To identify and analyze network activity, Content Security Reporter allows you to collect and manage the data from your integrated alert, authentication, email, and web devices.

Use the collected data to identify these potential issues:

- Bandwidth overload
- Liability exposure
- Productivity loss
- Security threats

Once identified, you can use the information to modify your policies and effectively enhance network protection.

How Content Security Reporter works

Content Security Reporter uses several elements that work together to provide reporting capabilities.

To successfully set up, use, and maintain Content Security Reporter, understand the role for each of the Content Security Reporter elements.

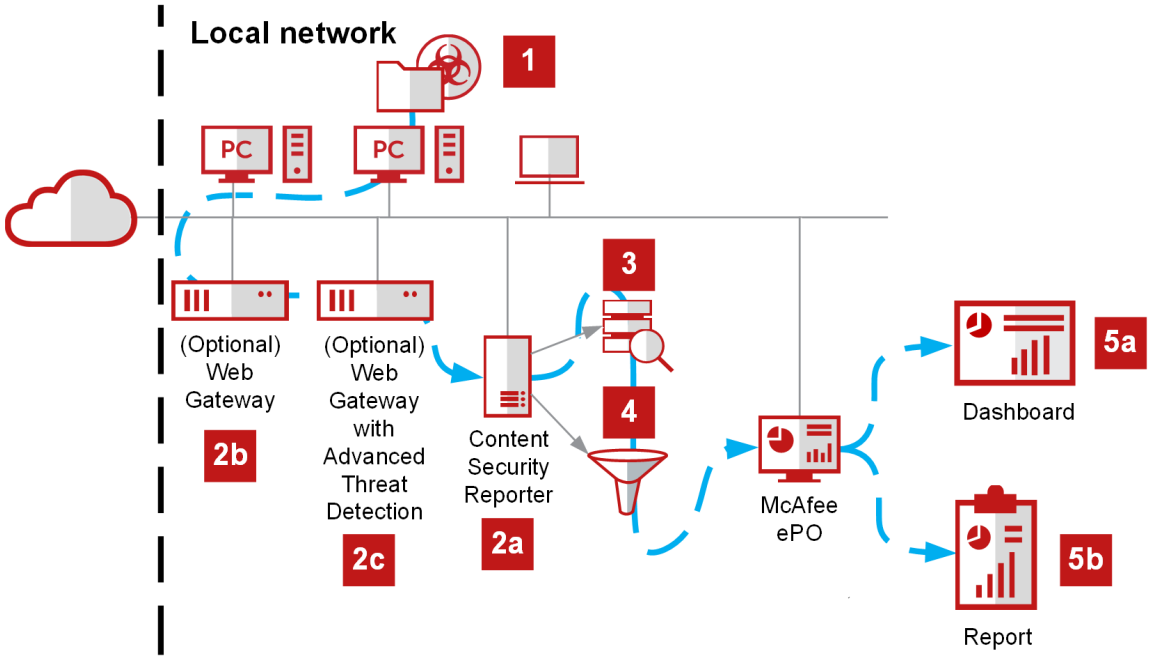

Figure 1-1 Content Security Reporter workflow

Content Security Reporter Number	Description
1	On managed systems, an alert or event occurs. Depending on your configuration, the alert or event is logged to the Content Security Reporter database.
2a	The Content Security Reporter database saves the alert, authentication, email, and web data.
2b	Web Gateway captures and logs the web event. It sends the logs to the Content Security Reporter database.
2c	Advanced Threat Defense captures and logs the event. It sends the logs to the Content Security Reporter database.
3	A Content Security Reporter query retrieves data from its database and defines how it is displayed.
4	A Content Security Reporter filter limits the data to specific users, websites, and threat reputations. The data is displayed in the McAfee ePO.
5a	Dashboard — Organizes your data in a customized view to provide detailed information for analysis.
5b	Report — Combines queries, filters, and other elements into a PDF to provide detailed information for analysis.

2 Changes in McAfee ePO

After you set up Content Security Reporter, all standard McAfee ePO features and functions are available, as well as additional Content Security Reporter changes that occur on the McAfee ePO interface.

To effectively use and maintain Content Security Reporter, understand the role for each of the following options.

Table 2-1 Changes to McAfee ePO

Option	Definition
Analytics	Enable analytics on dashboards for additional filter and workflow options.
Content Security Reporter permissions	Configure access and usage rights to Content Security Reporter features using McAfee ePO user permission sets.
Content Security Reporter dashboards	A set of default Content Security Reporter dashboards are installed that can be used as is, or duplicated and customized.
Content Security Reporter reports	A set of default Content Security Reporter reports are installed that can be used as is, or duplicated and customized.
Content Security Reporter queries	A set of default Content Security Reporter queries are installed that can be used as is, or duplicated and customized. Content Security Reporter queries can be added to other McAfee ePO dashboards and reports, not just those installed by Content Security Reporter.
McAfee® Common Catalog	Create and maintain groups of Common Catalog definitions such as domain names, network addresses, and network ports.
Reporting extensions	View and manage Content Security Reporter extensions.
Report Server	The report server provides McAfee ePO with Content Security Reporter features. The report server and Content Security Reporter database server are added at the same time. McAfee recommends you do not change the default database server settings.
Report Server Settings	Manage the server status, log sources, databases, maintenance tasks, and system utilities.

3 Report server settings

Use the report server settings to manage and configure the options that define the log data used in reports and how Content Security Reporter performs.

Contents

Directories

Content Security Reporter uses directories to retrieve user and group information.

Contents

When to use the internal directory

By default, Content Security Reporter installs with an internal directory. Use the internal directory when you need to store a local list of your network users and groups.

Use the internal directory for these scenarios:

- The network does not have an external directory.
- A separate directory is needed to store user names and groups.

The internal directory is unable to support nested groups.

When to use external directories

Content Security Reporter uses the McAfee ePO external directories.

For information on McAfee ePO directories, refer to the *McAfee ePolicy Orchestrator Product Guide*.

Content Security Reporter supports these external directories:

- Active Directory
- OpenLDAP

Log sources

Content Security Reporter uses log sources to collect the data displayed in dashboards and reports.

Log source modes

Log sources modes depend on the ability of your network filtering device to send log data to Content Security Reporter.

You can configure a log source by importing a single log file, or by using these options:

- **Accept incoming log files** — Content Security Reporter accepts log data from network filtering devices.
- **Collect log files from** — Content Security Reporter collects log data from network filtering devices or log data storage devices.

Log formats

Log formats determine how Content Security Reporter processes (also called *parsing*) data from log files, and how the data is stored in the database.

Content Security Reporter recognizes the structure of auto-discover and fixed-field log formats.

User-defined columns

Up to four user-defined columns can be configured for each log source during log file processing, and can be used to substitute column data, or to obtain data from columns that are normally skipped.

User-defined columns are also used when repopulating database columns during database maintenance.

User-defined columns do the following:

- Include skipped log field data — During log file processing, some log file fields are skipped. For example, log file processing skips the McAfee® Web Gateway **Referrer** and **Policy name** fields. Up to four user-defined columns are available to pull data from the skipped fields.
- Assign a custom value to column data — To easily find and review in reports, substitute standard column data with a custom string value. For example, you want to assign *test-lab* to all IP addresses beginning with *115*, and assign *other* to any additional IP addresses. In the report, the user-defined column displays either *test-lab* or *other* in place of the numeric IP address values. Content Security Reporter treats newly created user-defined columns as an additional column and leaves the original column and data in the log file. Using the previous example of substituting IP addresses, the original IP address column data remains unchanged and is still available to use in reports.

When entering a value in the **Log file header** value box, do not use quotation marks.

Processing and post-processing

When configuring a log source, use the **Processing** and **Post-Processing** tabs to determine how Content Security Reporter handles the data pulled from log files.

Page views setting

The **Condense log records into page views** setting on the **Processing** tab for a log source affects queries and disk space requirements for the reporting database.

Each line of a log file is a separate HTTP request for a webpage element. Viewing one webpage can result in multiple records in the log file.

The **Condense log records into page views** option consolidates multiple records from a log file into a single page view, or "hit," in reports. Condensing log records into page views generates a concise report view when using either summary or detailed queries. For example, condensing log records into page views could potentially reduce a 1 GB log file to a 100 MB log file.

By default, the **Condense log records into page views** option is enabled. If you disable this option, each webpage you visit, and element on the page, are logged as separate HTTP requests. For example, if you visit www.example.com, which contains multiple elements, the log data generates as follows:

www.example.com

www.example.com/rss.xml

www.example.com/advertisement.js

adserver.example.com/ad1.jpg

adserver.example.com/ad2.jpg

adserver.example.com/ad3.jpg

When you enable **Condense log records into page views**, your log data will show only one HTTP request as a page view —*www.example.com*.

Directory

Directories collect the group information for users that are located in the log file.

When you select multiple directories, Content Security Reporter prioritizes the directories as they appear in the **Selected directories** list.

If the configured directories are Secure Sockets Layer (SSL) enabled, you might experience slowness in parsing logs.

Custom columns

Custom columns substitute the data in the browser and cache columns in your log files with a word or phrase that better identifies the browser or cache value.

Custom columns are pre-defined rules. Instead of your reports containing *Mozilla/4.0 (compatible; MSIE 7.0...)*, the reports contain *Internet Explorer 7.0*. However, the original data value is retained in your database.

Each custom column uses a configured rule set to substitute technical data values from the browser or cache columns, and substitute with common identifiers to make the browser and cache data in your reports more recognizable.

Custom rule sets

Rule sets are customized instructions that tell Content Security Reporter to look for a specific string of data during log file processing and replace it with a different string. This resulting string appears in reports and is more recognizable to users. A test function is available to validate the result of a rule set.

Rule sets make your custom columns and user-defined columns work. Configure rule sets to find any string that appears in a log file and replace it with a different string defined by you. The string can be letters, numbers, and symbols.

Custom column rule sets

Custom columns are predefined for the browser and cache columns. Each custom column has a corresponding rule set. You can modify the rule sets, but you cannot add or delete rule sets for the custom columns.

User-defined column rule sets

User-defined columns are customized by you for any available log record or header. You create the rule sets for these columns, which can be edited, deleted, copied, and used by more than one user-defined column at a time.

Browse time

You can specify the length of time for the browse time threshold.

Content Security Reporter estimates a user's browse time by calculating the difference between the time stamps of two log lines.

For example, if the log file shows that Jon Lock visits www.example.com at 03:00:00 p.m. and news.example.com at 04:30:00 p.m., the browse time is the 1 hour 30 minutes that occurred between the time he visited www.example.com and news.example.com. However, Jon Lock probably did not spend more than one hour viewing a single webpage. To compensate for this, Content Security Reporter overrides the estimated browse time with a default browse time.

The browse time threshold option specifies the maximum length of time you expect a user to spend viewing a single webpage. The default is three minutes. When a user exceeds the browse time threshold, the default browse time is recorded in the database instead.

Databases

Content Security Reporter uses a database to store data from log files and is installed with an internal database, or you can use a supported external database. Set up a database that is appropriate for the size of your organization and the amount of data your organization generates.

Contents

When to use an internal database

During installation, Content Security Reporter is automatically configured to use the internal database (MariaDB 10.1.17).

The internal database installs on the same drive as Content Security Reporter.

Use the internal database for these situations:

- Small- to medium-size organizations
- Evaluating Content Security Reporter

Best Practice: You must have enough free drive space to accumulate data in the internal database. Only use the internal database when you need to store up to 50 GB of data.

Log files and data from the internal database are not transferable to another database.

When to use an external database

When your organization has more than 50 GB of data to store, Content Security Reporter requires a separate external database outside of the database already installed for McAfee ePO.

McAfee recommends using an external database for the following situations.

- There is more than 50 GB of data to store
- In a medium- to large-size organization
- Do not want to condense log records into page views
- Need to increase performance
- Need additional database management tools

To store report data, connect Content Security Reporter to one of the following supported external database platforms.

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- MySQL 5.5
- MySQL 5.6
- MySQL 5.7

Refer to the product documentation for your external database for instructions about backing up the database.

View the server status

View status information about the report server.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Server Status**.

3 Click **Refresh**.

Configure the directory

Use the default internal directory, or connect Content Security Reporter to the external directory on your network.

Content Security Reporter does not support Chase referrals and Global Catalogs.

Contents

Populate the internal directory

Import the UTF-8 encoded text file that Content Security Reporter uses to populate the internal directory.

Task

1 Create the UTF-8 encoded text file.

   a Open a new text file, then enter the user and group information.

   The user and group names must not contain spaces.

   Example:

```
group ENG

user bcarlisle

user jlock

group SALES

user jshepherd

user jfourd
```

   b Save the file on your computer.

2 Import the text file.

   a Select **Menu** | **Configuration** | **Report Server Settings** | **Directory**.

   b From the **Directory Name** list, select the internal directory.

   c Click **Actions**, then select **Edit**.

   d On the **General** tab, click **Choose File**, select the text file, then click **Open**.

   e Click **Import**.

   To make changes to the internal directory, open the text file, make your changes, then import the changed text file to Content Security Reporter.

3 Schedule when the internal directory retrieves user and group information.

   a Click the **Schedule** tab.

   b Configure the options.

   c Click **OK**.

Manually sync an external directory

The McAfee ePO directory automatically syncs with Content Security Reporter. If necessary, you can resync the external directory manually.

Task

See the *McAfee ePolicy Orchestrator Product Guide* to configure the external directory.

1 Select **Report Server Settings** | **Directories**.

2 Select the McAfee ePO directory.

3 Click **Actions**, then select **ReSync**.

Configure log sources

Configure the log sources that collect the data used in dashboards and reports.

- The fields displayed on the **Source** tab differ depending on which option you choose.
- Approximately 1 GB of temporary space is needed on the Content Security Reporter server for every GB of log data collected and processed.

Task

1 Choose the log source mode and format.

a Select **Menu** | **Configuration** | **Report Server Settings**.

b From the **Setting Categories** menu, select **Log Sources**.

c From the **Actions** menu, select **New**.

d On the **New Log Source** page, type a name for the log source and configure the remaining options.

2 Configure user-defined columns.

a Click the **User-Defined Columns** tab.

b Select the **Populate this column** checkbox.

c Select and configure up to four user-defined columns.

- If the log record is not found in the **Log record** drop-down list, use the **Log file header** field to define a header.
- When entering a value in the **Log file header** field, avoid using quotation marks.

3 Create a schedule for processing logs.

The **Schedule** tab is only available when the **Collect log files from** mode is selected.

a Click the **Schedule** tab.

b Specify the frequency, date, and time.

4 Configure processing and post-processing options.

a Click the **Processing** or **Post-Processing** tabs.

b Configure the options.

5 Configure the directories.

a Click the **Directory** tab.

b From the **Available directories** list, select the directories, then click **Add**.

6 Click **OK**.

Create a McAfee Network Security Manager MySQL account

Create the MySQL database user account that Content Security Reporter uses to access McAfee® Network Security Manager log sources.

McAfee recommends that you create a MySQL database user account specifically for communication between Content Security Reporter and McAfee Network Security Manager.

Task

1 Locate the McAfee Network Security Manager MySQL installation folder.

Example: C:\Program Files (x86)\McAfee\Network Security Manager\MySQL

a Open a command prompt and type:

```
cd <MySQL installation folder>\bin
```

b Press **Enter**.

2 Log on to MySQL.

a On the command prompt, type:

```
mysql --user=root mysql -p
```

b Press **Enter**.

c When prompted, type your password.

3 Create the user account.

a On the command prompt, type:

```
CREATE USER 'user_name'@'<ip_address>' IDENTIFIED BY 'some_password';
```

b Press **Enter**.

4 Grant permissions to the account for the appropriate database and tables.

a On the command prompt, type:

```
GRANT SELECT ON <database_name>.* TO 'user_name'@'<ip_address>';
```

- The default `<database_name>` is `lf`.
- <ip_address> is the Content Security Reporter server IP address.

b Press **Enter**.

For more information about adding user accounts, see the *MySQL 5.0 Reference Manual*.

Configure Advanced Threat Defense log sources

To collect McAfee® Advanced Threat Defense data, configure the Web Gateway and Advanced Threat Defense log sources.

Before you begin

Content Security Reporter uses Web Gateway to collect Advanced Threat Defense scan result data. Before you configure Advanced Threat Defense log sources, verify that the Advanced Threat Defense settings are configured on Web Gateway.

Task

1 To create each log source, follow these steps:

   a Select **Menu** | **Configuration** | **Report Server Settings**.

   b From the **Setting Categories** menu, select **Log Sources**.

   c From the **Actions** menu, select **New**.

   d In the **New Log Source** page, enter the unique log source name in the **Name** field.

   e Verify that the **Enable log source** checkbox is selected.

2 To configure the Web Gateway log source, choose from one of these options.

Table 3-1 Web Gateway log source configuration options

Task	Steps
Enable Content Security Reporter to accept incoming Web Gateway log files.	1 From the **Mode** drop-down list, select **Accept incoming log files**, then select one of these options: • **FTP / HTTP(S)** • **Syslog** 2 From the **Log format** drop-down list, select **McAfee Web Gateway (Webwasher) - Auto Discover**. 3 Configure the settings on the available tabs, then click **OK**.
Enable Content Security Reporter to collect log files from Web Gateway.	1 From the **Mode** drop-down list, select **Collect log files from**, then select one of these options: • **McAfee Web Gateway 6.x (Webwasher)** • **McAfee Web Gateway 7.x** 2 Configure the **Web Gateway Server** settings, then click **Test**. 3 If the settings are correct, configure the settings on the remaining tabs, then click **OK**.

3 To configure the Advanced Threat Defense log source, choose from one of these options.

Table 3-2 Advanced Threat Defense log source configuration options

Task	Steps
Enable Content Security Reporter to accept incoming Advanced Threat Defense log files.	1 From the **Mode** drop-down list, select **Accept incoming log files**, then select one of these options: • **FTP / HTTP(S)** • **Syslog** 2 From the **Log format** drop-down list, select **McAfee Web Gateway (MATD) - Auto Discover**. 3 Configure the settings on the remaining tabs, then click **OK**.
Enable Content Security Reporter to collect log files from Advanced Threat Defense.	1 From the **Mode** drop-down list, select **Collect log files from** | **McAfee Web Gateway 7.x (MATD)**. 2 Configure the **Web Gateway Server** settings, then click **Test**. 3 If the settings are correct, configure the settings on the remaining tabs, then click **OK**.

Check the status of running logs

To check the logs that are currently processing, view the list of running jobs.

Task

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources**.

3 Click the **Current Jobs** tab.

4 To update the status of jobs currently running, click **Refresh**.

Check the statistics for processed logs

View the statistics for logs processed by Content Security Reporter.

Task

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources**.

3 Click the **Statistics** tab.

4 To update the **Cumulative log statistics** or **Syslog client statistics**, click Refresh.

Manage log processing jobs

Manage the list of log processing jobs that are queued, running, or completed.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources** | **Job Queue**.

3 From the **Actions** menu, select a task you want to perform.

Modify custom column rule sets

Modify the data string sets for the corresponding custom columns used during log file processing.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources** | **Custom Columns**.

3 From the **Actions** list, select **Edit Rule Set**.

4 On the **Edit Rule Set** page, select **New** from the **Actions** menu.

5 On the **New Rule** page, type the data string value in the **Replace** field.

6 From the **With** drop-down list, choose any additional characters, then click **OK**.

Create user-defined column rule sets

Create custom rule sets for the user-defined columns used during log file processing.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources** | **Custom Rule Sets**.

3 From the **Actions** menu, select **New**.

4 Enter a name and description for the rule set.

5 Add a data string to the **Rules** list.

   a From the **Actions** menu, select **New**.

   b From the **New Rule** page, type the data string value in the **Replace** field.

   c From the **With** drop-down list, choose any additional characters, then click **OK**.

Configure browse time options

Choose the threshold and default time for estimated browsing session lengths.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources** | **Browse Time**, then click **Edit**.

3 On the **Edit Browse Time** page, select the time in minutes from the **Browse time threshold** drop-down list.

4 From the **Default browse time** drop-down list, select the time in minutes, then click **Save**.

Import a single log file

Import log files from a directory on the client computer.

To avoid errors, verify that the log file format matches the log source in your imported log files.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Log Sources**.

3 Select a log source.

4 From the **Actions** menu, select **Import Log**.

5 On the **Import Log** page, click **Browse**, find the log file you want to import, then click **Open**

A message confirms that the selected log file is imported.

6 Click **OK**.

Content Security Reporter processes the log file, and the status appears on the **Current Jobs** tab.

Configure the database

McAfee Content Security Reporter is installed with an internal database, or you can use a supported external database.

Contents

Connect to the internal database

Connect to the internal database that is installed with Content Security Reporter.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Reporter Server Settings**.

2 From the **Setting Categories** menu, select **Database**.

3 In the **Configuration** section, select **Default internal database**.

Connect to an external database

To store the data for your medium- to large-size organization, connect Content Security Reporter to a supported external database.

If the Content Security Reporter and McAfee ePO databases share the same SQL Server instance, you must configure separate databases for each.

- Users on the Microsoft SQL Server database must have db_owner permissions.
- You can install Content Security Reporter and the external database on the same computer, or on separate computers. If Content Security Reporter is installed on the same computer as the external database, there must be enough disk space to accumulate large amounts of data.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Reporter Server Settings**.

2 From the **Setting Categories** menu, click **Database**.

3 On the **Database** page, select **Edit**.

4 From the **This external database** drop-down list, select the database.

5 On the **Database settings** configuration area, enter the database information.

6 To verify that the database information is correct, click **Test**.

A status message indicates success or failure.

7 Click **Save**.

The connected external database appears as the database server in the **Registered Servers** list: **Menu** | **Configuration** | **Registered Servers**. McAfee recommends that you do not edit the settings on the **Registered Servers** page.

Configure performance options

Configure the performance options to ensure that Content Security Reporter runs efficiently.

Contents

Edit memory allocation

Dedicate the amount of memory available to the report server.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Performance Options**.

3 In the **Memory** section, click **Edit**.

4 Enter the amount of memory to allocate.

For 32-bit:

- Minimum memory value — 1024 MB
- Maximum 32-bit memory value — 1536 MB

For 64-bit:

- Minimum memory value — 3072 MB

Exceeding the maximum memory value causes negative performance issues.

5 Click **OK**.

Configure the amount of concurrently running jobs

View and configure the maximum amount of log processing jobs that can run simultaneously.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Performance Options**.

3 In the **Concurrent jobs** section, click **Edit**.

4 From the **Maximum concurrent log processing jobs** drop-down list, select a value, then click **OK**.

McAfee recommends using the default value of 2.

Manage the log processing cache

To monitor the effectiveness of cache sizes, and determine log processing memory requirements, view and configure the settings for the log processing cache.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Performance Options** | **Cache**.

The log processing cache table appears.

3 Edit the cache settings.

   a From the table, select a cache.

   b From the **Actions** menu, select **Edit**.

   c Configure the settings, then click **OK**.

Manage the log processing summary cache

View and manage the settings for the cache that holds the summary log processing data.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Performance Options** | **Summary Cache**.

   The summary log processing cache table appears.

3 Edit the summary cache settings.

   a From the table, select a summary cache.

   b From the **Actions** menu, select **Edit**.

   c In the **Maximum Entries** field, enter the value, then click **OK**.

4 Reporting

Use dashboards to identify and analyze your organization data, and report your findings using preconfigured or customized reports.

Contents

Monitoring with dashboards

Dashboards allow you to watch and monitor the data collected within your organization, and find relationships between the data to help you prevent risks in your network environment.

The following additional options are available for Content Security Reporter dashboards.

- **Dashboard Visibility** — Controls which users in your organization are able to view specific dashboards
- **Analytics** — Enables additional filter and pivot actions so you can further customize and analyze your data

Default dashboards

Content Security Reporter comes with a set of default dashboards that you can run as they are, or duplicate and customize to suit your needs.

Default dashboards are available from the **Dashboards** tab and contain data obtained from Content Security Reporter default or customized queries. Dashboards display information such as:

- Email activity
- Web hybrid activity
- Web policy enforcement
- Productivity
- IPS security overview

Custom dashboards

Create a dashboard, or duplicate and customize an existing dashboard for a specific and focused view of your organization's data.

For additional custom options, enable advanced analytics from the **New Dashboard** and **Edit Dashboard** windows. Enabling analytics provides you the following additional options:

- **Filtering** — Add additional filters to focus in on which data you want to display on a dashboard and within a specified time range.
- **Pivot** — For specific log record information, navigate from a configured monitor on the dashboard layout to another dashboard focused around the same log record information.
- **Table and chart legends** — Select data within a chart or table legend to view or remove data.

Monitors

Dashboards are collections of monitors. You can tailor dashboard information by adding monitors that provide specific Internet and email usage, and IPS alert information.

A monitor displays data from default or custom queries in the form of charts and tables. Each monitor is configured independently in order to display multiple combinations of your organization's data.

Querying the database

Content Security Reporter allows you to create and run queries and reports that provide Internet and email usage, and IPS alert data in the form of charts and tables. The data for these queries and reports is pulled from log data, and is stored in the registered internal or external database.

Use any of the default queries and reports, or duplicate and modify existing queries and reports to create your own for a customized view of your organization's data.

Queries

To collect your organization data, run queries individually, or combine them within dashboards and reports to view a broader range of data.

Content Security Reporter includes default queries that you can run as is, or create a customized query for your specific reporting needs.

Query Builder

Content Security Reporter provides a four-step wizard to create queries or to duplicate and customize default queries. Use the wizard to configure which data is retrieved and how it is displayed.

Custom query result types

Query result types identify where the data is retrieved from and what type of data is retrieved.

Each query result type provides its own set of data options (also called columns) to select from. The query type determines the amount of detail available for generating reports. The following query result types are available to you:

- **Detailed Email Delivery** — Data based on the delivery status of sent emails
- **Detailed Email Detection** — Information regarding viruses detected in sent and received emails
- **Email Summary** — High-level email usage information
- **Detailed Alert Data** — Detailed information about alerts generated from IPS devices

- **Detailed Advanced Threat Defense Data** — Detailed information about files scanned by Advanced Threat Defense
- **Detailed Web Access** — Represents web traffic details such as full request URLs and exact date and time of each request
- **Web Summary** — Generation of hourly data for reports such as hits per user, categories per week, bytes per log source, and more
- **Detailed Authentication Data** — Detailed information about McAfee® One Time Password (McAfee OTP) authentication events

It is quicker to generate reports and queries that are based on summary data than detailed data.

Custom query charts

Content Security Reporter provides a number of layout options to display the data it retrieves. Choose from various layout options to best display your data.

Custom query columns

Query columns determine the type of data to retrieve from the database and the order in which the data is displayed.

Custom query-level filters

Specify criteria by selecting properties and operators to limit the data retrieved by the query.

Query-level filters filter data only for the query in which they are applied.

For example, you already have a query that shows the top sites visited within your organization. To show only the top sites visited by user *jsmith*, you would select the **Username** column and type *jsmith* in the **Value** column property field. The results of the query will generate the top corresponding sites to the user *jsmith*.

Use column properties to filter data only when report-level filters cannot be used.

When you want more filtering capabilities and control over data in all queries — such as hourly, weekly, or monthly versions of the same queries — use report-level filters.

Reports

Content Security Reporter includes highly customizable, flexible, and easy-to-use reporting capabilities.

Reports are customizable documents that display data from one or more Content Security Reporter elements in a single PDF document for focused and offline analysis.

Use the **Report Builder** to create and run reports that display charts and tables with user-configured data. The most recently run report is stored within Content Security Reporter and readily available for viewing.

Default reports

Content Security Reporter installs several default reports made of Content Security Reporter queries and filters. Default reports are available from Content Security Reporter Shared Groups.

Default reports produce data from Content Security Reporter summary and detailed queries, for example:

- Your users' Internet activity
- The most blocked websites, malware, and applications

- The most used websites and applications
- Potential security threats to your organization

Custom reports

Create a custom report, or duplicate and customize a default report to suit your needs.

The following display and setting options are available to customize your reports:

- **Report data** — Information found within a report is based on the data generated within queries.
- **Format options** — Using these options, you can modify and customize various elements in the report format.
- **Runtime information** — Using these options, you can add specific runtime information to your report.

Delegated Reports

Delegated Reports is an access control feature to restrict which report data a user account can access.

In default reporting, users can view report for all users or groups. Using Delegated Reports under Permission Sets in McAfee ePO, administrators can configure which report data is available based on user names, user groups, IP address, or log sources. For more information about McAfee ePO permission set, see the product guide of your version of McAfee ePO.

When you select **All report data** in one permission set and **Selected report data** in other permission set, **All report data** takes precedence.

After creating permission sets, if the Content Security Reporter is removed and reinstalled, the user must enable those permissions again. To do this, the user must edit and save each permission set.

If you change the Permission Sets settings for a McAfee ePO user, the changes are effective from the next session when the McAfee ePO user logs in again.

Types of filters

Delegated Reports provides three types of filters:

- **Users/Groups**
- **IP Addresses**
- **Log Sources**

Users or Groups

Users can view data from all users and groups or only selected users and groups. The filters are case insensitive except User Groups. The user names are listed in lowercase. The user group name is displayed in bold. You can also include data from the log sources that do not have user names by enabling the **Include Anonymous** option. These users are displayed as dash.

When you select **Only selected users & groups** in Select Report Data, you can configure these options as required:

- **Search Database** — Displays users and group data from the logs that are processed previously.
- **Search Directory** — Allows you to search users and groups from the directory.
- **Add Manually** — Allows you to add users and groups manually.

By default, the maximum record fetching limit for Active Directory is 1000 and OpenLDAP is 500. If the number of records mentioned in the Find Now field exceeds the limit, only records within the limit are displayed. You can change the maximum limit by configuring the **MaxPageSize for AD**. For more information, see *Increase the MaxPageSize in Active Directory manually*.

You can add multiple permission sets to one user. When you include the user in one permission set and exclude from another permission set, exclusion takes precedence.

IP Addresses

Users can view data from all IP addresses or from only selected IP addresses. It supports both IPv4 and IPv6 format. You can also define one IP address or a range of IP address using the **Add Manually** option.

When you select **Only selected IP addresses** in the Select Report Data, you can configure these two options as required:

- **Search Database** — Displays all IP addresses from the logs that are processed earlier.
- **Add Manually** — Allows administrators to add IP address or IP addresses range manually.

Log Sources

Log Sources displays the configured log sources that you can use for reporting.

Users can view data from all log sources or from only selected log sources. If the logs in the Report server are deleted but already parsed, those logs are also included in the list.

Using multiple Permission Sets for one user

Administrators can assign more than one Permission Sets to users.

The following table explains how Permission Sets work for different scenarios when administrators assign more than one Permission Sets.

Permission Set 1 configuration	Permission Set 2 configuration	Expected result
All report data	**Selected report data**	User can view all report data.
Selected report data | **All users & groups** | **All IP addresses** | **All log sources**	**Selected report data**, specific user in **Only selected users & groups** , **Single IP address** in **Only selected IP address**, and specific log source in **Only selected log source**.	User can view report data from all IP addresses, all log sources for all users.
Selected report data with `user_1` included.	**Selected report data** with user_1 excluded.	User can't view report data from `user_1`.
Selected report data with `user_1` included, **Include anonymous** is selected for **All IP addresses**, and **All log sources**.		User can view report data only from `user_1` and anonymous users.
Selected report data with `user_1` that is part of `group_1` included, **Include Anonymous** is selected, exclude `group_1` for **All IP addresses**, and **All log sources**.		User can view report data only from anonymous users.
Selected report data with `user_1` that is part of `group_1` excluded, and `group_1` included for **All IP addresses**, and **All log sources**.		User can view report data only from `group_1` user data except `user_1` data.
Selected report data with `user_1` included, deselect **Include Anonymous**, **All IP addresses** and **All log sources**.		User can view report data only from `user_1` data.
Selected report data with `group_1` included for **All IP addresses**, and **All log sources**.		User can view report data only from `group_1` data.

Permission Set 1 configuration	Permission Set 2 configuration	Expected result
Selected report data with `group_1` excluded, for **All IP addresses** and **All log sources**.		User can view report data for all users and groups except `group_1` users.
Selected report data with `user_1` and `group_3` excluded, for **All IP addresses**, and **All log sources**.		User can view report data for all users and groups except `user_1` and `group_3` users.
Selected report data with no users or groups selected, **Include Anonymous** deselected for **All IP addresses**, and **All log sources**.		User can view report data for all users and groups except Anonymous data
Selected report data with `user_1` selected, `user_3` excluded, **Include Anonymous** deselected, **Add IP range** defined, and log source `mwg_1` is selected.		User can view report data for `user_1` for the IP address range from the `mwg_1` log source. Data from `user_3` and other IP addresses are excluded.
Selected report data with `user_1` (a source user of NSM log) selected, `user_3` (destination user of NSM log) excluded, **Add IP range** defined, and log source `nsm_1` selected.		User can view NSM report data with `user_1` as source and destination within the IP range, includes data from `nsm_1` log, and excludes `user_3` and other users with other IP address and also from other NSM log source if any.
Selected report data with **Include Anonymous** selected.	**Selected report data** with **Include Anonymous** deselected.	User can view reports for data except anonymous data.

Increase the MaxPageSize in Active Directory manually

Increase the MaxPageSize manually.

Task

1 Type `LDAP policies` at the Ntdsutil.exe command prompt in the Active Directory, then press **Enter**.

2 Type `set maxpagesize to <number>`, then press **Enter**.

For example, to set the maximum record size to 7000, type `set maxpagesize to 7000`.

3 Type `Show Values`, then press **Enter** to verify the changes.

4 Type `Q`, then press **Enter** to quit.

Configure a dashboard

Create a dashboard that allows you to see your organization's data and how you want to see it.

Create a dashboard

Set up customized dashboards to view your organization's Internet and email usage, and IPS alert data.

Task

For option definitions, click **?** in the interface.

1 Add a dashboard to Content Security Reporter.
   a On the menu bar, click **Dashboards**.
   b In **Dashboard Actions**, click **New**, and type a name for the dashboard that allows you to easily identify it.
   c In **Dashboard Visibility**, select who can view this dashboard.
2 Enable additional filtering capabilities.
   a In **Analytics**, select **Enabled**.
   b From the drop-down list, select a filter.
   c Click **OK**.

Add monitors to dashboards

Add monitors to a dashboard for a customizable view of your data.

> **Before you begin**
> You must have write permissions for the dashboard you are modifying.

Every monitor type supports different configuration options. For example, a query monitor provides the option to modify the query, database, and refresh interval.

Task

1 Select **Menu** | **Reporting** | **Dashboards** and select a dashboard.
2 Click **Add Monitor**.

   The **Monitor Gallery** appears at the top of the screen
3 From the **View** drop-down list, select a query.

   The available monitors in that category appear in the gallery.
4 Drag the monitor onto the dashboard. As you move the cursor around the dashboard, the nearest available drop location is highlighted. Drop the monitor into the location you want.

   The **New Monitor** dialog appears.
5 Configure the monitor as needed (each monitor has its own set of configuration options), then click **OK**.
6 After you have added monitors to this dashboard, click **Save Changes** to save the newly configured dashboard.
7 When you have completed your changes, click **Close**.

Tasks

- *Filter dashboard data* on page 32
  Use filters to further customize the data in dashboard tables and charts.
- *Pivot options* on page 33
  Use monitors to drill down and view specific data information, then use the pivot options to create, or view a different dashboard.
- *Add data to Common Catalog lists* on page 33
  Use Common Catalog as a central data repository for IP addresses, sites, and user names.
- *View Global Threat Intelligence information* on page 34
  View McAfee® Global Threat Intelligence™ information to assess threats from malware, URLs, and IP addresses.
- *View a site* on page 34
  From your dashboard data, drill down to access data URLs and view the associated websites.

Filter dashboard data

Use filters to further customize the data in dashboard tables and charts.

Before you begin

Filter options are only available when analytics is enabled on a dashboard.

Task

1 Select **Menu** | **Reporting** | **Dashboards**.

2 Add a filter to the dashboard.

Table 4-1 Filter dashboard data

To...	Follow these steps...
Add your own filter.	1 Click **Add Filter**. 2 Select the **Filter Type** and enter the **Filter Value**. 3 Click **OK**. In the **Filter Value** field, you can enter the filter pattern using these wildcard values: • Asterisks (*) — Used to match one or more characters. For example, `*a*` matches all filter type results containing `a`. • Question marks (?) — Used to match one character. For example, `?jones` matches all filter type results beginning with any one character and ending with `jones`. You can use multiple question marks for the **Filter Value**.
From a monitor, filter the data.	1 Click the arrow next to the data item you want to remove from the dashboard. 2 From the drop-down list, select **Add Filter**.
View specific data by minutes, hours, or days.	1 In the **Show last** field, enter a number value. 2 From the drop-down list, select a frequency. 3 Click **Go**.

The applied filter appears in the **Add Filter** area of the dashboard.

Pivot options

Use monitors to drill down and view specific data information, then use the pivot options to create, or view a different dashboard.

Before you begin

Pivot options are only available when analytics is enabled on a dashboard.

Task

1 Select **Menu** | **Reporting** | **Dashboards**.

2 To create or view a different dashboard, choose from one of these options.

Table 4-2 Pivot options

To...	Follow these steps...
Pivot from the dashboard	1 Click the arrow next to the data item. 2 From the drop-down list, select **Pivot to**.
Pivot from the **Details** page	1 Click a data point. *Example*: On a bar chart, select a bar of data. 2 On the data table, select the row of data you want to view. 3 On the **Details** page, select a highlighted data item, then select **Pivot to** from the drop-down list.

Add data to Common Catalog lists

Use Common Catalog as a central data repository for IP addresses, sites, and user names.

Before you begin

To create a catalog list, select **Menu** | **Common Catalog**.

Common Catalog does not support IPv6 addresses.

Task

1 Select **Menu** | **Reporting** | **Dashboards**.

2 To add data to Common Catalog lists, choose from one of these options.

Table 4-3 Common Catalog options

To...	Follow these steps...
Add data to Common Catalog from the dashboard	1 Click the arrow next to the data item. 2 From the drop-down list, choose one of these options: • **Add to List** — Deposits the data item into a **Common Catalog** list. • **Remove from List** — Removes the data item from a **Common Catalog** list. To select multiple lists, press **Ctrl** or **Shift**, then select the appropriate lists.
Add data to Common Catalog from the **Details** page	1 Click a data point. *Example*: On a bar chart, select a bar of data. 2 On the data table, select the row of data you want to view. 3 On the **Details** page, select a highlighted data item, then select one of these options from the drop-down list: • **Add to List** — Deposits the data item into a **Common Catalog** list. • **Remove from List** — Removes the data item from a **Common Catalog** list. To select multiple lists, press **Ctrl** or **Shift**, then select the appropriate lists.

View Global Threat Intelligence information

View McAfee® Global Threat Intelligence™ information to assess threats from malware, URLs, and IP addresses.

Task

1 Select **Menu** | **Reporting** | **Dashboards**.

2 To view Global Threat Intelligence data, choose from one of these options.

Table 4-4 Global Threat Intelligence view options

To...	Follow these steps...
View Global Threat Intelligence data from the dashboard	Click the arrow next to the data item, then select **View GTI info** from the drop-down list.
View Global Threat Intelligence data from the **Details** page	1 Click a data point. *Example*: On a bar chart, select a bar of data. 2 On the data table, select the row of data you want to view. 3 On the **Details** page, select a highlighted data item, then select **View GTI info** from the drop-down list.

View a site

From your dashboard data, drill down to access data URLs and view the associated websites.

Before you begin

View site options are only available when analytics is enabled on the dashboard.

Task

1 Select **Menu** | **Reporting** | **Dashboards**.

2 To view a site, choose from one of these options.

Table 4-5 Site view options

To...	Follow these steps...
View a site from the dashboard	Click the arrow next to the data item, then select **View site** from the drop-down list.
View a site from the **Details** page	1 Click a data point. *Example*: On a bar chart, select a bar of data. 2 On the data table, select the row of data you want to view. 3 On the **Details** page, select the highlighted URL, then select **View site** from the drop-down list.

Configure queries

Configure queries to retrieve the data Content Security Reporter uses to generate reports.

View Top Users by Browse Time example:

When configuring a query, consider the following user scenario for viewing the top users in your organization by overall browse time.

Assume the users in your organization have access to the Internet, and you would like to block specific users from the sites they visit most often.

Use the **View Top Users by Browse Time** query to compare which users in your organization use the most browse time. After you have identified which users in your organization use the most browse time, Content Security Reporter allows you to block these users from accessing their most visited websites.

In this scenario, you are able to:

- Discover which users in your organization use the most browse time.
- Compare the users in your organization that use the most browse time.
- Assess the websites top users visit most often.
- Block the websites that the top users visit most often.

Task

1 Select the query result type.

a Select **Queries & Reports** | **Actions** and click **New**, or select an existing query from the list and click **Edit**.

The **Query Builder** appears with the **Result Types** view active.

b From the **Database Type** drop-down list, select **Content Security Reporter**.

c From the **Feature Group** list, select an option.

The associated data types appear on the **Result Types** menu.

d Select a result type, then click **Next**.

2 Select the query layout.

   a From the **Display Results As** menu, select a layout to best display your data.

   b Configure the remaining layout options, then click **Next**.

   When entering the maximum value for the display, it is recommended to use a lower value. For example, when configuring the **Grouped Bar Chart** options, type 10 instead of 200 in the **Maximum groups** field.

3 Select the query columns.

   a From the **Available Columns** menu, select the columns to apply to your query.

   b In the **Selected Columns** configuration area, select, drag, and position each column data type.

   c Click **Next**.

4 From the **Available Properties** menu, select which properties to use for filtering your query and the appropriate values for each.

5 Click **Run** to check that you get the type of results you expect.

   If the query returns unexpected results, click **Edit Query** and edit the query options.

6 Save the query.

   a Click **Save**.

   b On the **Save Query** page, type a name for the query, add any notes, and select the group.

   c Click **Save**.

Tasks

- *Track group membership* on page 36
  Configure Content Security Reporter to pull a list of groups from the directory during log file processing and directory updates.

Track group membership

Configure Content Security Reporter to pull a list of groups from the directory during log file processing and directory updates.

Task

1 Configure the directory group attribute.

   a Select **Menu** | **Configuration** | **Report Server Settings**, then click **Directories**.

   b Select the directory, then click **Actions** | **Copy**.

   c Click the **Advanced** tab, enter the **Group Key**, then click **OK**.

   d On the **Directories** page, select the directory, then click **Actions** | **Update Now**.

2 Add the directory to the log source.

   a Click **Log Sources**, then select the log source.

   b Click **Actions** | **Edit**.

   c On the **Edit Log Source** page, click the **Directory** tab.

d From the **Available directories** list, select the directory, then click **Add**.

e Click **OK**.

3 Configure the query.

a Select the **Result Type**, then click **Next**.

b From the **Chart type** menu, select **List** | **Table**, then click **Next**.

c From the **Available Columns** list, select **Group List**, then click **Next**.

Best Practice: Only use the **Group List** when you change the query settings. Avoid the **Group List** option when you create a new query.

d From the **Available Properties** list, select **Group Filter**, then click **Run**.

Best Practice: Only use the **Group Filter** to track group membership.

Run reports

Generate a report using default or customized queries. For example, create a report that shows the top blocked malware in your organization using data available from your configured queries.

Before you begin

By default, you must have administrator rights to be able to view, modify, and run existing reports as well as add new reports. To give other users the ability to create and run reports, select **Menu** | **User Management** | **Permission Sets** and edit the **Content Security Reporter** permission for each user type.

If the report includes runtime parameters, you can specify those parameters when running the report.

Task

1 Select a query.

a Select **Queries & Reports** | **Actions** | **Report** and click **New**, or select an existing report from the list and click **Edit**.

The Report Builder opens with the **Report Layout** view active.

b From the toolbox, drag a query chart to the report layout configuration area.

The **Configure Query Chart** dialog box opens.

c Select the available query options.

d Click **OK**.

2 Customize the report.

a In the **Name, Description and Group** tab, type a name, description, and which group to use.

Use the **Header and Footer** and **Page Setup** tabs to specify how you want the query to appear in the report.

b Use the **Runtime Parameters** tab to select report-level filters.

3 Click **Run** to generate the report.

At this point, you can choose to run the report to get the information immediately, save to use it another time, configure its appearance further by adding additional content.

View Advanced Threat Defense reports

To further analyze Advanced Threat Defense data, register the Advanced Threat Defense server and view the analysis reports.

Contents

Register the Advanced Threat Defense server

To view the Advanced Threat Defense analysis results, register the Advanced Threat Defense server with McAfee ePO.

Task

1 Create the Advanced Threat Defense server.
   a Select **Menu** | **Configuration** | **Registered Servers**, then click **New Server**.
   b On the **Registered Server Builder** page, select **MATD server** from the **Server type** drop-down list.
   c In the **Name** field, enter the unique Advanced Threat Defense server name.
   d In the **Notes** field, enter any additional information, then click **Next**.
2 Configure the Advanced Threat Defense server settings.
   a In the **Server Name or IP Address** field, enter the Advanced Threat Defense server name or IP address found on the Web Gateway interface.
   b In the **User name** field, enter your Advanced Threat Defense user name.
   c In the **Password** field, enter your Advanced Threat Defense password.
   d Click **Test Settings**.
   e If the settings are correct, click **Save**.

View the Advanced Threat Defense reports

To view and download the Advanced Threat Defense reports, drill down from the dashboard monitor to the **Details** page.

Before you begin

Advanced Threat Defense reports are only available from queries configured for Advanced Threat Defense content.

Task

1 From your Advanced Threat Defense dashboard monitor, select a data point.

2 In the data table, select the row of data you want to view.

3 On the **Details** page, click **MATD Analysis Reports**, then select one of these options:

- **View Analysis Summary (PDF)** — Downloads a PDF file that contains an executive brief detailing key behaviors of the sample file
- **View Complete Results** — Downloads a .zip file that contains all available Advanced Threat Defense reports for an analyzed sample

Schedule queries and reports

Create a schedule to regularly run queries and reports.

Task

1 Select **Menu** | **Automation** | **Server Tasks**.

2 From the **Actions** menu, select **New Task** to open the Server Task Builder on the **Description** page.

3 Type a name for the task, and use the **Notes** area to add any additional information such as the expected results. Select whether you want the task enabled or disabled, and click **Next** to move to the **Actions** page.

4 From the **Actions** drop-down list, select **Run Query** or **Run Report**.

5 Select the query or report, its language, and whether you want to export the contents to a file, or send it to someone else, or run another command.

If you are exporting to a file, you must specify a destination directory before you can continue.

6 Click **Next** to move to the **Schedule** page.

7 Use the options to specify when you want the query or report to run, and for how long.

8 Configure any report-level filters.

9 Click **Next** to view a summary of the query or report settings.

10 Click **Save**.

The query or report is available to view, run, or edit from the **Server Tasks** list.

5 Content Security Reporter maintenance

Content Security Reporter requires regular maintenance to promote optimal performance and to protect your data. Database maintenance options allow you to perform tasks that optimize database performance and free database space. Over time, records are added to the database and more space is used. To free space in the database, you can delete older records you no longer need.

System maintenance options allow you to configure tasks that remove system status information and server logs to reduce disk space usage.

McAfee recommends that you perform database maintenance tasks during off-peak times. During maintenance, the database and new queries and reports are not available. Make sure you read the instructions for each maintenance task before starting the maintenance job in Content Security Reporter.

Contents

Maintain the database

Schedule database maintenance tasks to run at a regular frequency and start time, or perform the tasks manually for immediate results.

Contents

Configure automated database maintenance jobs

Configure the settings for when Content Security Reporter performs database maintenance jobs.

Task

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Database Maintenance**.

3 Click **Edit**, and configure these options:

- **Schedule database maintenance** — Create a schedule for when to run database maintenance jobs.
- **Delete database records** — Create database space by deleting database records.
- **Index maintenance** — Configure the frequency for when Content Security Reporter rebuilds indexes.
- **Maintenance options** — Specify the maximum number of records that are deleted at any one time.

Best Practice: Make sure that the database maintenance jobs occur at different times than the directory updates.

4 Click **Save**.

Run manual database maintenance jobs

Manually run database maintenance jobs for immediate results.

Contents

Delete database records by date range

Manually delete all database records within a specific date range.

Perform maintenance during off-peak times. Reports, queries, and dashboards are not available during maintenance.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Database Maintenance** | **Manual Maintenance**.

3 From the **Manual database maintenance by date range** section, select one of these options:

- **Delete summary and detailed records**
- **Delete summary records**
- **Delete detailed records**

4 Select the date range, then click **Start**.

5 When the **Confirm Maintenance** message appears, click **Yes**.

6 When the **Maintenance Job Status** message appears, click **OK**.

The database maintenance process is immediately queued.

Delete database records by log source

Delete database records for a specific log source when the data is no longer needed.

Perform maintenance during off-peak times. Reports, queries, and dashboards are not available during maintenance.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Report Server Settings**.
2. From the **Setting Categories** menu, select **Database Maintenance** | **Manual Maintenance**.
3. From the **Manual database maintenance by log source** section, select a log source from the drop-down list.
4. Click **Start**.
5. When the **Confirm Maintenance** message appears, click **Yes**.
6. When the **Maintenance Job Status** message appears, click **OK**.

   The database maintenance process is immediately queued.

Repopulate columns

Repopulate custom and user-defined columns to apply settings to existing database records.

Perform maintenance during off-peak times. Reports, queries, and dashboards are not available during maintenance.

Substituting Specific IP Addresses example:

Assume you have created a user-defined column to substitute specific IP addresses with the custom string value *test-lab* and now you have existing database records you want to apply to your created user-defined column.

Use the **Repopulate Columns** dialog box to repopulate the user-defined columns. By repopulating the columns, the specified IP addresses in existing database records now appear with the custom string value *test-lab*.

In this scenario, you are able to:

- Identify which specific IP addresses to substitute.
- Apply the custom string value *test-lab* to existing database records.
- Update database records by repopulating columns.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Report Server Settings**.
2. From the **Setting Categories** menu, select **Database Maintenance** | **Manual Maintenance**.
3. From the **Custom and user-defined columns section**, click **Repopulate Columns**.
4. Configure the options for **Custom columns** and **User-defined columns**, then click **OK**.

5 When the **Confirm Maintenance** message appears, click **Yes**.

6 When the **Maintenance Job Status** message appears, click **OK**.

The re-populate columns process is immediately queued.

Rebuild indexes

Perform manual index rebuilding when you want to rebuild the indexes immediately.

Perform maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Database Maintenance** | **Manual Maintenance**.

3 From the **Index Maintenance** section, click **Rebuild Indexes**.

4 When the **Confirm Maintenance** message appears, click **Yes**.

5 When the **Maintenance Job Status** message appears, click **OK**.

The database maintenance process is queued immediately.

Run database statistics

View database statistics without performing maintenance.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Database Maintenance** | **Manual Maintenance**.

3 Click **Run Statistics**.

4 When the **Confirm Maintenance** message appears, click **Yes**.

5 When the **Maintenance Job Status** message appears, click **OK**.

The database statistics process is immediately queued.

Manage database maintenance jobs

View and manage completed database maintenance jobs.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Database Maintenance** | **Status**.

3 From the **Actions** menu, choose from these options:

- **Cancel** — Stop Content Security Reporter from processing the selected database maintenance jobs.
- **Delete** — Remove the selected database maintenance jobs from the **Status** list.
- **Delete All Completed Jobs** — Remove all completed database maintenance jobs from the **Status** list.
- **Refresh** — Update the **Status** list with current running database maintenance jobs.

Maintain the system

Schedule system maintenance tasks to run at a regular frequency and start time, or perform the tasks manually for immediate results.

Contents

Configure automated system maintenance jobs

Configure the settings for when Content Security Reporter performs system maintenance jobs.

The report server is unavailable during scheduled system maintenance.

Task

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **System Maintenance**.

3 Click **Edit**, and configure these options:

- **Schedule system maintenance** — Set a time for when Content Security Reporter performs daily system maintenance.
- **Delete system status** — Configure the age of system status information and server logs to delete during daily system maintenance.

4 Click **Save**.

Run manual system maintenance jobs

Manually run system maintenance jobs for immediate results.

Task

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **System Maintenance** | **Manual Maintenance**.

3 To delete system status, select a time range, then click **Delete Now**.

4 When the **Maintenance Job Status** message appears, click **OK**.

The database maintenance process is immediately queued.

Manage system maintenance jobs

View and manage all system maintenance jobs.

Task

1 **Menu** | **Configuration** | **Report Server Settings**

2 From the **Setting Categories** menu, select **System Maintenance** | **Status**.

3 From the **Preset** drop-down list, select which system maintenance jobs to view.

4 From the **Actions** menu, choose from these options:

- **Delete** — Remove the selected system maintenance jobs from the **Status** list.
- **Delete All Completed Jobs** — Remove all completed system maintenance jobs from the **Status** list.
- **Refresh** — Update the **Status** list with current running system maintenance jobs.

Collect system information for troubleshooting

Should you require assistance with Content Security Reporter, generate a feedback file that contains system information that can be sent to McAfee technical support for troubleshooting purposes.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Setting Categories** menu, select **Support**.

3 Click **Start**.

4 When the **Support** message appears, click **OK** to continue.

A status message is generated when the file has been created.

The feedback files are stored in the report server installation directory.

System backup

When a backup configuration file is created, Content Security Reporter automatically saves the report server settings, which can be used to restore Content Security Reporter to an earlier configuration.

The backup configuration file does not create a backup of any reports, queries, or McAfee ePO settings.

The saved configuration settings include:

Settings	Description
Database connection settings	Saves the configuration settings that allow McAfee Content Security Reporter to communicate with the database.
Database maintenance settings	Saves scheduled database maintenance job settings and status messages.
General settings	Saves log source configuration and browse time settings.

Settings	Description
Performance settings	Saves database and system performance settings.
System status message	Saves log parsing job history and database maintenance settings.

Back up configuration settings

Create a backup file to restore configuration settings after upgrading the Content Security Reporter software, recover from a system failure, or move settings from one installation to another.

If you plan to use a backup file after uninstalling and re-installing Content Security Reporter, save the backup file to a location other than the Content Security Reporter installation directory.

Task

For option definitions, click **?** in the interface.

1. Select **Menu** | **Configuration** | **Report Server Settings**.
2. From the **Setting Categories** menu, select **System Backup**.
3. From the **Actions** menu, select **Backup Now**.

   When the System Backup message appears, click **OK**.

The backup process can take several minutes. A backup123456789 folder is created where 123456789 is the time stamp. By default, the folder is created in C:\Program Files\McAfee\Content Security Reporter\reporter \conf\. A backup.xml file is saved in the backup folder. To simply create a backup file, you can wait until the file is created, then continue working without restoring it.

Restore configuration settings

Restore the configuration settings to return to a previous state, or after the software is re-installed.

The backup folder and backup file must have read and write permissions for the same account running Content Security Reporter.

Task

1. Close McAfee ePO.

   If you need to re-install the previous version of Content Security Reporter that you were running, use the Microsoft Windows Programs and Features to remove Content Security Reporter, and then re-install the previous version of Content Security Reporter.

2. Stop Content Security Reporter services.
3. Go to your backup folder (by default, C:\Program Files\McAfee\Content Security Reporter\reporter\conf\) to locate the backup file that was created.

   - If a backup folder already exists, do not create a new one.

4 Copy the backup file from the backup123456789 folder to the backup folder in the conf directory.

If you re-installed Content Security Reporter, copy these files and directories you backed up to the corresponding locations in the C:\Program Files\McAfee\Content Security Reporter\reporter\ directory:

- .../conf/
- .../mysql/var/reporting/
- .../docs/

5 Restart Content Security Reporter.

6 Log on to McAfee ePO.

Execute an SQL statement

When working with technical support, the reporting administrator can execute SQL statements that safely query the database while troubleshooting.

Task

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 From the **Settings Categories** menu, select **Database**.

3 Click **Edit**.

4 Click **Execute SQL**.

The **Execute SQL** dialog box appears.

5 In the **Input** field, enter your SQL statement, then click **Run**.

6 To exit the dialog box, click **OK**.

A Auto-discover log formats

Content Security Reporter supports some auto-discover log formats. However, some modifications to the log file headers might be necessary to correctly parse the data.

The following tables provide necessary header modifications for the available auto-discover log formats:

- Blue Coat
- McAfee Web Gateway

This table provides information on Blue Coat log file headers used in Content Security Reporter and the necessary modifications to correctly parse the data. Some cells remain intentionally empty.

Table A-1 Blue Coat header formats

Format in extended log file	Custom	Content policy language	Description
c-ip	%a		IP address of the client.
cs-bytes			Number of bytes sent from client to appliance.
cs-categories			All content categories of the request URL.
cs-categories-bluecoat			All content categories of the request URL that are defined by Blue Coat Web Filter.
cs-categories-external			All content categories of the request URL that are defined by an external service.
cs-categories-local			All content categories of the request URL that are defined by a local database.
cs-categories-policy			All content categories of the request URL that are defined by CPL.
cs-categories-provider			All content categories of the request URL that are defined by the current third-party provider.
cs-categories-qualified			All content categories of the request URL, qualified by the provider of the category.
cs-category			Single content category of the request URL (such as sc-filter-category).
cs-host	%v		Host name from the client's request URL. If URL rewrite policies are used, this field's value is derived from the log URL.

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
cs-method			Request method used from client to appliance.
cs-request-line			First line of the client's request.
c-dns	%h		Host name of the client (using the client's IP address to avoid reverse DNS).
cs-uri		• url • log_url	• Original URL requested • The log URL
cs-uri-address		• url.address • log_url.address	• IP address from the original URL requested. DNS is used if the URL is expressed as a host name • IP address from the log URL. DNS is used if URL uses a host name
cs-uri-categories			All content categories of the request URL.
cs-uri-categories-bluecoat			All content categories of the request URL that are defined by Blue Coat Web Filter.
cs-uri-categories-external			All content categories of the request URL that are defined by an external service.
cs-uri-categories-local			All content categories of the request URL that are defined by a local database.
cs-uri-categories-policy			All content categories of the request URL that are defined by CPL.
cs-uri-categories-provider			All content categories of the request URL that are defined by the current third-party provider.
cs-uri-categories-qualified			All content categories of the request URL, qualified by the provider of the category.
cs-uri-category			Single content category of the request URL (such as sc-filter-category).
cs-uri-host		• url.host • log_url.host	• Host name from the original URL requested • Host name from the log URL
cs-uri-hostname		• url.hostname • log_url.hostname	• Host name from the original URL requested. RDNS is used if the URL is expressed as an IP address • Host name from the log URL. RDNS is used if the URL uses an IP address

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
cs-uri-path	• *blank* • %U	• url.path • *blank*	• Path of the original URL requested without query • Path from the log URL without query
cs-uri-pathquery		• url.pathquery • log_url.pathquery	• Path and query of the original URL requested • Path and query from the log URL
cs-uri-port		• url.port • log_url.port	• Port from the original URL requested • Port from the log URL
cs-uri-query	• *blank* • %Q	• url.query • *blank*	• Query from the original URL requested • Query from the log URL
cs-uri-scheme		• url.scheme • log_url.scheme	• Scheme of the original URL requested • Scheme from the log URL
cs-uri-stem			• Stem of the original URL requested • Stem from the log URL The stem includes everything up to the end path, but does not include the query.
cs-user	%u		Qualified user name for NTLM; relative user name for other protocols.
cs-userdn			Full user name of a client authenticated to the proxy (fully distinguished).
cs-username			Relative user name of a client authenticated to the proxy (not fully distinguished).
date	%x	date.utc	GMT date in YYYY-MM-DD format.
gmttime	%t		GMT date and time of the user request in [DD/MM/YYYY:hh:mm:ss GMT] format.
localtime	%L		Local date and time of the user request in [DD/MMM/YYYY:hh:mm:ss +nnnn] format.
rs(Content-Type)	%c	response.header.Content-Type	Response header: Content-type.
sc-bodylength			Number of bytes in the body (excludes header) sent from appliance to client.

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
sc-bytes	%b		Number of bytes sent from appliance to client.
sc-filter-category	%f		Content filtering category of the request URL.
sc-filter-result	%W		Content filtering result: Denied, Proxied, or Observed.
sc-headerlength			Number of bytes in the header sent from appliance to client.
sc-status	%s		Protocol status code from appliance to client.
time	%y	time.utc	UTC (GMT) time in HH:MM:SS format.
timestamp	%g		Unix type time stamp.
x-cache-user			Relative user name of a client authenticated to the proxy (not fully distinguished, same as cs-username).
x-client-address			IP address of the client.
x-client-ip			IP address of the client.
x-cs-dns		client.host	The host name of the client obtained through reverse DNS.
x-cs-http-method		http.method	HTTP request method used from client to appliance. Empty for non-HTTP transactions.
x-cs-user-authorization-name		user.authorization_name	User name used to authorize a client authenticated to the proxy.
x-cs-user-credential-name		user.credential_name	User name entered by the user to authenticate to the proxy.
x-cs-user-login-address		user.login.address	The IP address that the user was authenticated in.
x-cs-username-or-ip			Used to identify the user using either their authenticated proxy user name, or if that is unavailable, their IP address.
x-sc-http-status		http.response.code	HTTP response code sent from appliance to client.
x-virus-id		icap_virus_id	Identifier of a virus if one was detected.

This table provides information on McAfee Web Gateway log file headers used in Content Security Reporter and the necessary modifications to correctly parse the data.

Table A-2 McAfee Web Gateway header formats

Header	Description
"attribute"	URL categories.
"auth_user"	Client user name.
"auth_user_anonymous"	Anonymous user name.
block_res	Filtering action.

Table A-2 McAfee Web Gateway header formats *(continued)*

Header	Description
bytes_to_client	Number of bytes written to the client.
bytes_from_client	Number of bytes received from the client.
bytes_to_server	Number of bytes sent to the web server from McAfee Web Gateway.
bytes_from_server	Number of bytes received from the web server.
"categories"	URL categories.
elapsed_time	Time to process request.
"media_type"	Content-type header.
"profile"	Skipped.
"referer"	Referer.
"rep_level"	Reputation of the URL.
"req_line"	Request.
src_host	Client host name.
src_ip	Client IP address.
status_code	HTTP status code.
time_stamp	Time of request.
unix_epoch	UNIX time stamp.
"user_agent"	Client user agent.
"virus_name"	Name of virus found in the request.

B Fixed-field log formats

Some supported fixed-field log formats do not require any header changes. Content Security Reporter correctly parses the data from these log files without any modifications.

The following table provides information about supported log file formats that are not automatic-discover in Content Security Reporter. This table includes examples of the expected header information found in the corresponding log file format.

Any deviation from the expected field format can result in inaccurate reports.

Table B-1 Non-automatic-discover log file formats

Log file type	Expected formats	Examples
McAfee SaaS Web Protection Service	"user_id", "username", "source_ip", "http_action", "server_to_client_bytes", "client_to_server_bytes", "requested_host", "requested_path", "result", "virus", "request_timestamp_epoch", "request_timestamp_formatted", "uri_scheme", "category"	"47877615", "user1@webreporter.com", "192.168.0.1", "GET", "664", "2837", "www.myspace.com", "/", "DENIED", "", "1319501356", "2011-10-24 18:09:16-06", "http", "Social Networking"
McAfee Email and Web Security Format (Web)	tv_sec.(tv_usec/1000) cache_msec client_ip cache_code/http_code cache_size method_str url user hier_code/hier_host content_type sf_action "sf_cats"	1085754420.626 1 192.168.0.1 TCP_DENIED/403 0 GET http://www.msn.com/ sjones ONE/- - DENY "Portal Sites"
McAfee SiteAdvisor Enterprise Format	DetectedUTC EventTypeID CategoriesShortName URL ActionID RatingID ReasonId AgentGUID User MachineName PhishingFacet DownloadsFacet SpamFacet PopupsFacet BadlinkerFacet ExploitFacet IP MIMEType	2009-01-01T14:31:12 18600 rb http://www.0d6b214a-aafe-42e9-a150-c237c86cd959.com/a9cf15e0-c151-408a-a8b2-fb31debd8e7c.html 1 1 9 ef4a3a5b-773b-467f-af1f-f1ddb0f5ba31 sara machine1 6 3 6 6 1 6 192.168.0.1 text/html
McAfee Firewall Enterprise (Sidewinder) SFv4 - Text Format	client_ip - user_1 [time_stamp] "GET url" http_status sf_action sf_cats	192.168.0.1 - jlock [28/Jun/2004:11:44:54] "GET http://www.msn.com" 403 COACH "Portal Sites"
McAfee SmartFilter IFP SFv4 - Text Format	client_ip - user_1 [time_stamp] "GET url" http_status sf_action sf_cats	192.168.0.1 - imanderson [28/Jun/2004:11:44:54] "GET http://www.msn.com" 403 COACH "Portal Sites"

Index

M

O

P

Q

R

S

T

U

V

W