Data Usage Statement

Revision C

McAfee Web Gateway

Contents

- About this document
- What McAfee uses collected data for
- Starting data collection
- Updates
- File rating
- Malware scanning
- Dynamic content classification
- Policy configuration

About this document

This document provides information about the data that is collected for product improvement when you are running McAfee® Web Gateway (Web Gateway).

What McAfee uses collected data for

McAfee uses data collected when running Web Gateway for analyzing web-related threats to improve the security functions of the product. The data is also used for improving performance and other capabilities of the product.

The collected data includes, for example, URLs that Web Gateway categorized when users of your network submitted them for web access or names of malware programs that requested web objects were found to be infected with.

The data is transferred from Web Gateway to McAfee servers and retrieved from them as feedback.

The feedback functions are enabled in Web Gateway by default. We recommend that you leave them enabled and participate in the collection of data to allow us to analyze it for your own benefit and that of other customers.

If you do not want to participate, refer to the instructions provided in this document for disabling data collection.

Data protection measures

An encrypted channel is used to transfer collected data from Web Gateway to the McAfee servers.

Our personnel and that of our authorized partners are instructed to keep all data in a protected environment and to use it only for product improvement purposes.

Data collected

Data is collected and sent to the McAfee servers when the following functions are performed within Web Gateway.

- Updates
- URL categorization and rating
- File rating
- Malware scanning
- Dynamic content classification
- Policy configuration (beginning with version 7.5.1 of Web Gateway)

Different types of data are collected depending on the function. You can disable data collection for each function.

Starting data collection

To ensure data collection is only performed to the amount that you have configured, the collection process is not started before you have clicked the **Save Changes** button on the user interface.

This allows you to:

- Review the Data Usage Statement (this document) and select the checkbox for accepting it
- Configure the disabling of data collection for particular types of data on the user interface, as described in the following sections of this document
- Save these settings

Before you configure settings for data collection, you can work with the setup wizard to configure other initial settings. After finishing the wizard, you are asked whether you want to save what you have configured.

You should then wait with clicking **Save Changes** until you also have configured the settings for data collection.

Updates

Information for use by the filtering modules of Web Gateway (also known as filter engines) is updated in regular intervals on an appliance.

For example, updates are performed for DAT files containing virus signatures, for the URL filter database, or for Subscribed Lists, providing filtering information such as IP addresses or URLs.

When an update is performed, relevant data is collected and sent to the McAfee update servers, which take the role of feedback servers on these occasions.

The data is sent each time Web Gateway contacts an update server to retrieve new updates.

Data collected for updates

The following types of data are collected for updates.

- Product name, for example, *MWG*
- Version number, for example, *7.5.0*
- Build number, for example, *18062*
- License information, including the customer ID
- Operating system, for example, *MLOS (McAfee Linux Operating System)*
- Operating system subtype, for example, *mlos-1.0-x64*
- ID of the appliance Web Gateway is running on

  This is a uniquely and universally identifying string, known as *UUID*.
- Appliance model, for example, *WBG-5500-B*
- System management BIOS (DMI) appliance vendor, for example, *McAfee*
- System management BIOS (DMI) appliance model, for example, *Appliance A3*
- System management BIOS (DMI) serial number, for example, *J040209263*
- CPU type, for example, 4*Intel Core *i3 CPU 540 @ 3.07GHz*
- Memory size, for example, *3810724 KB*
- Network interface cards, for example, *4*igb, 1*e1000e*
- Telemetry and debug information, for example, the health status of an appliance
- Flag that indicates whether Helix proxy functions were enabled
- For each updatable filter engine:
  - Version number
  - Plugin version number
  - Faulty version number (if a version is faulty)
  - Troubleshooting information, for example, the reason that caused a version to become faulty

Disable data collection for updates

You can disable the collection of data about updates by disabling engine updates for an appliance on the user interface of Web Gateway.

Task

1. Select **Configuration | Appliances**, then select the appliance you want to disable engine updates for.
2. Click **Central Management**.
3. Scroll down to **Automatic Engine Updates** and deselect the following three checkboxes:
   - **Enable automatic updates**
   - **Allow to download updates from internet**
   - **Allow to download updates from other nodes**
4. Click **Save Changes**.

File rating

When a user requests the download of a file from the web, a lookup is performed to retrieve information that rates the file for its reputation.

The information is retrieved from the McAfee Global Threat Intelligence service, whose servers take the role of feedback servers, and relevant data is sent to these servers.

This data is sent each time a reputation lookup is performed for a file.

Data collected for file rating

The following types of data are collected for file rating.

- Name and version of the McAfee product involved in the scanning
- Name of the product component that scanned the file
- Version of the drivers that rated a file to be suspicious
- Version of the DAT file used for the scanning
- File hash

  This hash uniquely identifies a file if it exists in a McAfee database.
- Fingerprint

  This bit sequence indicates traits in a file structure that are common in malware.
- Environmental information

  This bit sequence indicates environment cues commonly associated with malware. The information is based on and restricted to data that the operating system stores about a file. It does not include the file name or content stored in the file.

Disable data collection for file rating

You can disable the collection of data about file rating by disabling in-the-cloud lookups on the user interface of Web Gateway.

Task

1. Select **Policy** | **Settings**.
2. Under **Engines** | **Anti-Malware** select the Anti-Malware settings you want to disable in-the-cloud lookups for.
3. Under **Advanced Settings** deselect **Enable GTI file reputation queries**.
4. Click **Save Changes**.

Malware scanning

When a web object, for example a web page or executable file, is scanned by the Gateway Anti-Malware (GWAM) engine and found to be infected with malicious content, relevant data is collected and sent to the McAfee servers involved in the scanning.

The data is sent each time malicious content is detected.

Data collected for malware scanning

The following types of data are collected for malware scanning.

- Product name, for example, *MWG*
- Version number, for example, *7.5.0*
- Time stamp
- HTTP method
- URL that was submitted by a user

  This does not include user name and password (if contained in the URL), nor any URL parameters.
- Occurrence count, specifying how often the malicious content was detected
- Name of the malware
- Content type
- Content hash
- Content length
- HTTP Referer Header
- HTTP User Agent Header

Disable data collection for malware scanning

You can disable the collection of data about malware scanning by configuring the feedback settings on the user interface of Web Gateway.

Task

1. Select **Configuration | Appliances**, then select the appliance you want to disable the collection of malware scanning data for.
2. Click **Telemetry**.
3. Deselect **Send feedback to McAfee about potentially malicious web sites**.
4. Click **Save Changes**.

Dynamic content classification

When a website has been rated by the McAfee Dynamic Content Classification (DCC) engine, relevant data is collected and sent to the McAfee servers involved in the rating.

The data is sent each time a new web site was rated.

Data collected for dynamic content classification

The following types of data are collected for dynamic content classification.

- Product name, for example, *MWG*
- Version number, for example, *7.5.0*
- Time stamp
- HTTP method
- URL that was submitted by a user

  This does not include user name and password (if contained in the URL), nor any URL parameters.
- Occurrence count, specifying how many instances of website access were evaluated
- Category the website was rated to fall into, for example, *Online shopping*
- Set of rules that determined a category

  For each rule that was involved, the rule name and the reputation score it provided for a website are specified.
- Version number of the rule package

Disable data collection for dynamic content classification

You can disable the collection of data about dynamic content classification by configuring the feedback settings on the user interface of Web Gateway.

Task

1. Select **Configuration | Appliances**, then select the appliance you want to disable the collection of data about dynamic content classification for.
2. Click **Telemetry**.

3 Deselect **Send feedback to McAfee about dynamically classified web sites**.

4 Click **Save Changes**.

Policy configuration

A security policy for web access from inside your network is implemented on Web Gateway.

To implement this policy web security rules are configured that are grouped in rule sets. The rules use lists and settings for the filter modules on Web Gateway that are known as engines, for example, the Anti Malware engine or the URL filter engine.

Data about the configured rules, lists, and settings of the policy is collected and sent to the McAfee servers.

Policy configuration data is collected beginning with version 7.5.1 of Web Gateway.

Disable collection of policy configuration data

You can disable the collection of policy configuration data by configuring the feedback settings on the user interface of Web Gateway.

Task

1 Select **Configuration** | **Appliances**, then select the appliance you want to disable the collection of policy configuration data for.

2 Click **Telemetry**.

3 Deselect **Send feedback to McAfee about policy information in order to improve the product**.

4 Click **Save Changes**.