## Contents

### 1 Introduction
- Welcome ........................................... 5
- About this guide .................................. 5
- What else will you find in this introduction? .. 6
- Using McAfee Web Gateway .................... 6
  - First-level tabs .................................. 7
  - Configuring a sample setting ............... 7
  - Standard features of the user interface ... 9
- McAfee Web Gateway user documentation ... 12
  - Documentation on main products .......... 13
  - Documentation on special products ....... 13
- McAfee Web Gateway product licenses ...... 14
  - New licensing model ......................... 14
  - Old licensing model ......................... 14
  - Importing licenses ......................... 15

### 2 Home
- Home features ................................... 17
- Dashboard ........................................ 17
  - Executive summary ......................... 22
  - Traffic volume ............................... 24
  - System .......................................... 26
  - McAfee Web Gateway ...................... 30
- Overview ......................................... 34
  - Overview ...................................... 34
- Support ........................................... 37
  - Support ......................................... 37
- TrustedSource ................................... 38
  - TrustedSource ................................. 38
  - Malware Feedback Black List ............ 42
  - URL Feedback Black List .................. 43
  - Feedback ....................................... 44
- Manuals .......................................... 45
  - Documentation on main products ........ 46
  - Documentation on special products ..... 47
  - Additional documentation ............... 48
- Preferences ..................................... 49
  - Preferences .................................... 49
- License .......................................... 52
  - Information .................................... 52
  - Notification ................................... 54

### 3 Common
- Common features ................................ 57
- Quick snapshot .................................. 57
- Quick snapshot .................................. 58
- Media type filters ............................... 61
  - Actions ......................................... 61
  - Media Type Black List ...................... 64
  - Media Type White List ...................... 65
- Document Inspector ............................. 67
  - Document Inspector ......................... 67
- Archive Handler ................................ 71
- Archive Handler ................................ 72
- Generic Header Filter ......................... 73
Contents

4 URL Filter
  Filtering web traffic .................................................. 113
  Quick snapshot ......................................................... 113
  Categories .............................................................. 115
  Web reputation ......................................................... 118
  URL filtering methods .................................................. 119
    URL filtering methods ............................................. 120
  Category actions ....................................................... 123
    Category actions .................................................. 124
    Category defaults ................................................ 126
    Configuring an exempting action ................................ 129
  Quotas and coaching .................................................. 130
    Quotas and coaching .............................................. 130
  Filter by expressions .................................................. 132
    Filter by expressions ............................................ 133
  Web reputation ......................................................... 135
    Web reputation .................................................... 136
  Extended List Manager ................................................. 137
    Extended List Manager ........................................... 138
  Category scheme ........................................................ 140
    Category scheme .................................................. 140
  Progressive lockout ................................................... 141
    Progressive lockout .............................................. 142
  GTI settings ........................................................... 143
    GTI settings ...................................................... 143
Welcome

Welcome to the McAfee® Web Gateway URL Filter Administration Guide. It provides you with the information needed to configure and use the McAfee Web Gateway URL Filter.

The McAfee Web Gateway URL Filter reduces non-business related surfing to a minimum by blocking certain categories of Web sites, for example, online shopping and entertainment, suppresses distractions such as banner ads and prevents downloads of files such as MP3. It stems the tide of bandwidth-intensive files such as streaming media, thus improving your business application performance.

The URL Filter effectively filters out offensive sites and prevents downloads of inappropriate files, thus minimizing the risk of legal liabilities such as breaches of copyright, sexual harassment and support of criminal activities.

About this guide

The following overview lists the chapters of this guide and explains briefly what they are about:

- **Introduction** (this chapter) — Provides introductory information.

- **Home** — Describes basic features that are available in addition to the features of the individual products that can be run as parts of McAfee Web Gateway.

- **Common** — Describes filtering features that are available in addition to the features of the individual products that can be run as parts of McAfee Web Gateway.

- **URL Filter** — Describes the filtering features that are specific to the URL Filter.
What else will you find in this introduction?

In addition to the overview that was given in the previous section, this introduction also:

- Explains how to handle the user interface that has been developed for working with McAfee Web Gateway, see Using McAfee Web Gateway
- Informs you about the other documents that are provided for users of McAfee Web Gateway, see McAfee Web Gateway user documentation
- Informs you about the licensing models that exist for this version of McAfee Web Gateway, see McAfee Web Gateway product licenses

Using McAfee Web Gateway

A user-friendly web solution has been developed as the user interface for working with the McAfee Web Gateway features. The interface looks like this:

The following sections provide some information to make you familiar with this interface. These sections:

- List the first-level tabs of this interface and explain their meanings, see First-level tabs
- Describe a sample procedure showing how a setting is configured for a McAfee Web Gateway feature, see Standard features of the user interface
- Explain more about some standard features of this interface, see Standard features of the user interface
First-level tabs

The user interface displays a number of tabs and sections for configuring the McAfee Web Gateway features. These tabs appear on the first level:

- Home, Common, URL Filter, Anti Malware, Anti Spam, SSL Scanner, User Management, Reporting, Caching, Proxies, and Configuration

They are used to complete the following tasks:

**Home, Common** – These tabs are for configuring basic and filtering features that are available in addition to the features of the individual products that can be run as parts of McAfee Web Gateway.

**URL Filter** – This is the first-level tab for configuring the features that are specific to the URL Filter.

The following tabs are not described in this document, see the corresponding guides for more information:

**Anti Malware, Anti Spam, SSL Scanner** – These tabs are for configuring the features of other individual McAfee Web Gateway products.

**User Management, Reporting, Caching, Proxies, Configuration** – These tabs are for configuring features that adapt McAfee Web Gateway as a whole to the system environment it is running in.

Note: The Anti Malware tab is used for both the McAfee Web Gateway Anti-Malware and Anti-Virus products.

Note: The Caching tab is only available when McAfee Web Gateway is run as an appliance.

For more information about these tabs, see the *McAfee Web Gateway System Configuration Administration Guide*.

Configuring a sample setting

This section explains how to configure a sample setting for a McAfee Web Gateway feature. The feature chosen here for explanation is the **Animation Filter**.

To avoid the download of bandwidth-consuming animated images, this filter detects and modifies or removes them. For this sample configuration, just suppose you want to enable the filter and let it remove any such images from the filtered objects. You also want these settings to be part of your default filtering policy.

These are the main steps needed for configuring the feature:

1. Navigate to the section
2. Configure settings
3. Make settings effective
In more detail, these steps include the following activities:

1. Navigate to the section
   a. Select the **Common** tab:

   ![Image of common tab]

   - **Policy:**
     - **default:**
     - **Media Type Filters**
     - **Document Inspector**
     - **Archive Handler**
     - **Generic Header Filter**
     - **Generic Body Filter**
     - **Advertising Filters**
     - **Privacy Filters**
     - **Text Categorization**
     - **HTTP Method Filter List**
     - **FTP Command Filter List**
     - **Welcome Page**
     - **White List**

   - **default** is selected in the line below **Policy**, which means that the settings you are going to configure now will be valid under your default filtering policy. So, leave this selection as it is.

   **Note:** Otherwise, you could select a different filtering policy, using the drop-down list provided here.

   b. In the navigation area on the left, select **Advertising Filters**, which is located under **Policy**:

   ![Image of advertising filters]

   c. Enable **Advertising Filters**. To do this, select the checkbox next to the inscription.

   You need to do this because all features that are placed under this main feature (including the Animation Filter) will only work if it is enabled.

   d. From the tabs provided for configuring the **Advertising Filters** options, select the **Settings** tab:

   ![Image of settings tab]

   The **Animation Filter** section is located on this tab:

   - **Animation Filter** - Manages and filters animated images
     - **Animated images:**
       - Show only the first picture of an animation
       - Repeat animation [ ] time(s)
       - Remove all animated images

   ![Image of animation filter settings]

   ![Image of animation filter settings details]
2 Configure settings
   a Enable the feature. To do this, select the checkbox next to the section heading.
   b Select the radio button labeled **Remove all animated images**.

   **Note:** To get help information on these settings, click the question mark in the top right corner of the section.

   The section should now look like this:

   ![Animation Filter](image)

3 Make settings effective
   Click **Apply Changes**.

   This completes the sample configuration.

### Standard features of the user interface

This section explains features that are provided in the user interface for completing standard tasks, such as applying changes to your settings or searching for a term on the tabs of the user interface:

- **Apply changes**
- **Click history**
- **Information update**
- **Logout**
- **Main feature enabling**
- **Search**
- **Session length**
- **System information**

**Apply changes**

After modifying the settings in one or more of the sections on a tab, you need to click **Apply Changes** to make effective what you have modified.

The **Apply Changes** button is located in the top right corner of the user interface area:

![Apply Changes](image)

When modifying settings that belong only to a particular filtering policy, you can make the modified settings apply to all policies, nevertheless.

An arrow is displayed next to the **Apply Changes** button on each tab where policy-dependent settings can be configured:

![Apply Changes](image)
Clicking this arrow will display a button, which you can use to apply changes to all policies:

Apply Changes to All Policies

When you are attempting to leave a tab after modifying its settings, but without clicking **Apply Changes**, an alert is displayed to remind you to save your changes:

```
Save changes?
Would you like to save your changes before leaving this page?
Yes  No  Cancel
```

Answer the alert by clicking **Yes** or **No** according to what you intend to do about your changes. This will take you to the tab you invoked before the alert was displayed.

Clicking **Cancel** will make the alert disappear, so you can continue your configuration activities on the current tab.

**Click history**

The tabs you visited while configuring settings are recorded on the top left corner of the user interface area. They are recorded together with the paths leading to them.

The current tab and path are always visible in the display field:

```
Common > Policy > Media Type Filters > Actions
```

Clicking the arrow to the right of the path display will show the click history — a list of the tabs you visited prior to this one:

```
Common > Policy > Media Type Filters > Actions
Common > Policy > Media Type Filters > Actions
Common > Policy > Advertising Filters > Settings
SSL Scanner > Quick Snapshot
Common > Quick Snapshot
Home > Dashboard > Executive Summary
```

Clicking any of the entries displayed in the list will take you to the corresponding tab.

**Note:** The click history is only recorded for the current session until you log out. After logging in to a new session, the recording of tabs and paths is reset.

**Information update**

Some parts of the information that is provided on the tabs of the user interface will change from time to time. In these cases, the information display is updated automatically every three seconds by McAfee Web Gateway.

So, you might have performed a manual update of the anti-virus engines. This means that the information provided in the **Current Status** and **Log File Content** sections on the corresponding **AV Engine** tab will begin to change continuously over a certain period of time until the update is completed.

These sections are then updated automatically every three seconds to reflect the status of the update process.

**Logout**

To logout from a McAfee Web Gateway session, click the **logout** link, which is located in middle position at the top of the user interface area.

After logging out, the login page is displayed, where you can login again and start a new session.
**Main feature enabling**

There are McAfee Web Gateway settings that can only be modified if a corresponding main feature is enabled. For example, if you want to modify the settings of the **Phishing Filter** section on the **Settings** tab under **Anti-Spam > Message Filters**, you need to make sure the **Message Filter** feature itself is also enabled.

If you attempt to modify settings while the corresponding main feature is not enabled, an alert is displayed to make you aware of this situation:

```
Your changes will have no effect, because the main feature is disabled
```

**Search**

A **Search** input field and button are located in the top right corner of the user interface area:

```
Search
```

You can start keyword queries of the entire user interface by entering a search term in the input field and clicking **Search**:

```
timeout
Search
```

The search output is presented in a separate window, which displays a list of the tabs the search term was found on and the paths leading to them:

```
The query for 'timeout' produces following output:
- Proxies > Web Proxies > HTTP Proxy
- Configuration > NTLM
- Configuration > AV Engine
- Configuration > CRLs
- Configuration > Master Settings
- Configuration > Central Management
- User Management > Import
- Home > Overview
- Configuration > Proactive Scanning
- Configuration > Sessions
- Configuration > Spam Filter
- Reporting > Overall Reporting > View Live Reports > System Statistics
- Configuration > Update Manager
```

Clicking any of the entries displayed in the list will take you to the corresponding tab.

**Note:** To be able to use the search function, make sure JavaScript is enabled on your system.
Session length
When working with the user interface, you need to mind the session length. This length can be configured
in the Session Options section of the Sessions tab under Configuration > Web Interfaces.
After modifying the interval specified there, click Apply Changes to make the modification effective.
When a session has timed out, the following notification is displayed:

Click OK to acknowledge the notification. After clicking a tab or button of the user interface, the login
window opens, where you can login again and start a new session.

System information
At the top of the user interface area, system information is provided on the current McAfee Web Gateway
session. This information includes:
• Version and build of the McAfee Web Gateway software
• Name of the system McAfee Web Gateway is running on
• Name of the user logged in for the current session, for example, Admin
• Role assigned to this user, for example, Super Administrator
• Permissions granted to this user, for example, read/write

McAfee Web Gateway user documentation
This guide belongs to a series of documents provided for users of McAfee Web Gateway. The following
sections give an overview of:
• The user documentation on the main products that can be run as parts of McAfee Web Gateway, see Documentation on main products
• The user documentation on McAfee Web Gateway products for special tasks and environments, see Documentation on special products

Note: The user documentation can be viewed after navigating to the Manuals tab of the user interface. It can
also be viewed on the Webwasher Extranet, which is provided by McAfee.
## Documentation on main products

The table below gives an overview of the user documentation on the McAfee Web Gateway main products:

<table>
<thead>
<tr>
<th>Document group</th>
<th>Document name</th>
<th>What about?</th>
</tr>
</thead>
<tbody>
<tr>
<td>General documents</td>
<td><strong>McAfee Web Gateway Deployment Planning Administration Guide</strong></td>
<td>Is McAfee Web Gateway suited to my environment?</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway Installation Guide</strong></td>
<td>How to install McAfee Web Gateway?</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway Quick Configuration Guide</strong></td>
<td>First steps to get McAfee Web Gateway running</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway System Configuration Administration Guide</strong></td>
<td>Features for configuring McAfee Web Gateway within the system environment</td>
</tr>
<tr>
<td></td>
<td>Advanced Configuration Guide</td>
<td>More sophisticated configuration tasks</td>
</tr>
<tr>
<td></td>
<td>Upgrade Guide</td>
<td>What should I know when upgrading to a new McAfee Web Gateway release?</td>
</tr>
<tr>
<td>Product documents</td>
<td><strong>McAfee Web Gateway URL Filter Administration Guide</strong></td>
<td>Features for configuring URL filtering policies</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway Anti-Virus Administration Guide</strong></td>
<td>Features for configuring anti-virus filtering policies</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway Anti-Malware Administration Guide</strong></td>
<td>Features for configuring anti-malware filtering policies</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway Anti-Spam Administration Guide</strong></td>
<td>Features for configuring anti-spam filtering polices</td>
</tr>
<tr>
<td></td>
<td><strong>McAfee Web Gateway SSL Scanner Administration Guide</strong></td>
<td>Features for configuring SSL-encrypted traffic filtering policies</td>
</tr>
<tr>
<td>Reference document</td>
<td><strong>McAfee Web Gateway Reference Guide</strong></td>
<td>Items concerning more than one individual product, for example, features for customizing actions or log files</td>
</tr>
</tbody>
</table>

## Documentation on special products

The following table gives an overview of the user documentation on the McAfee Web Gateway products for special tasks and environments.

<table>
<thead>
<tr>
<th>Document group</th>
<th>Document name</th>
<th>What about?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special environment documents</td>
<td><strong>Setting Up Webwasher on Microsoft ISA Server</strong></td>
<td>Setting up McAfee Web Gateway or a product running with it in a special environment</td>
</tr>
<tr>
<td></td>
<td><strong>Setting Up Webwasher with Blue Coat</strong></td>
<td>see above</td>
</tr>
<tr>
<td></td>
<td><strong>Setting Up NetCache with ICAP</strong></td>
<td>see above</td>
</tr>
<tr>
<td></td>
<td><strong>NTLM Agent Set-up Guide</strong></td>
<td>Setting up an additional McAfee Web Gateway product to enable authentication using the NTLM method on platforms other than Microsoft Windows</td>
</tr>
<tr>
<td></td>
<td><strong>HSM Agent Set-up Guide</strong></td>
<td>Setting up an additional McAfee Web Gateway product to enable use of HSM (High Security Module) device</td>
</tr>
<tr>
<td>Appliances documents</td>
<td><strong>McAfee Web Gateway Appliances Installation and Configuration Guide</strong></td>
<td>Installing and configuring the McAfee Web Gateway appliances</td>
</tr>
<tr>
<td></td>
<td><strong>Appliances Upgrade Guide</strong></td>
<td>What you should know when upgrading to a new release of the McAfee Web Gateway appliances</td>
</tr>
</tbody>
</table>
McAfee Web Gateway product licenses

With version 6.8.4 of McAfee Web Gateway, there is a change in the way that licenses may be obtained. This applies to the license mode, which changes from the old subscription model to a perpetual model. It also applies to the distribution of Web security features within the individual products that can be run as parts of McAfee Web Gateway and are covered by different licenses.

New licensing model

Under the new model, two different licenses may be obtained:

- **Web Security Module license** — This is the base license for McAfee Web Gateway. It is included by default when McAfee Web Gateway is purchased.

  The license covers all functions that are required to run McAfee Web Gateway as HTTP, HTTPS, or FTP proxy. It also includes the URL Filter and several basic filters, such as the Advertising Filter and the Privacy Filter, and furthermore the SSL Scanner and the McAfee Anti-Virus engine.

- **Web Anti-Malware Module license** — This license may be purchased in addition to the base license. It is an add-on item and cannot be used on its own.

  The license covers the anti-malware functions of the Proactive Scanning Filter.

  **Note:** These functions are not included in the McAfee Anti-Virus engine.

There is no limit in time to the validity of licenses obtained under this model. However, the databases that McAfee Web Gateway uses to deliver protection against threats arising from the Web need to be updated at regular intervals.

This is ensured through concluding an appropriate support contract. When a contract finishes without a prolongation, McAfee Web Gateway continues to be operative, using the existing versions of the databases.

For information on how the import of licenses under the new model affects existing installations of McAfee Web Gateway 6.8.3 and 6.8.4, see [Importing licenses](#).

Old licensing model

Under the old model, licenses could be obtained on a subscription basis for each of the individual McAfee products that could be run as parts of McAfee Web Gateway (formerly Webwasher) and delivered different Web security features.

**Note:** Licenses for version 6.8.4 of McAfee Web Gateway will still be available under this model for a limited period of time after its release.

The following individual products were each covered by a separate license under the old model:

- **McAfee Web Gateway URL Filter**

  Helps you boost productivity by reducing non-business related surfing to a minimum, thus curbing your IT costs. Suppresses offensive sites and prevents downloads of inappropriate files, thus minimizing risks of legal liabilities.

- **McAfee Web Gateway Anti-Malware**

  Offers in-depth security against all kinds of malicious code, such as aggressive viruses, potentially unwanted programs, spyware, day-zero attacks and blended threats not covered by traditional anti-virus and firewall solutions. The highly efficient anti-malware engine is used in combination with the Proactive Scanning filtering technology.

- **McAfee Web Gateway Anti-Virus**

  Combines the strength of multiple anti-virus engines concurrently scanning all Web and e-mail traffic. The Proactive Scanning filtering technology additional detects and blocks unknown malicious code, not relying on time-delayed virus pattern updates. This combination provides in-depth security against a multitude of threats while offering unmatched performance through use of the Anti-Virus PreScan technology.
**McAfee Web Gateway URL Filter 6.9 Administration Guide**

**Introduction**

McAfee Web Gateway product licenses

**McAfee Web Gateway Anti-Spam**

Offers complete protection of the central Internet gateway. The highly accurate spam detection filters stem the flood of unwanted spam mail before it reaches the user’s desktop. Your systems will not be impaired, the availability of valuable internal mail infrastructures, such as group servers, is thus maintained.

**McAfee Web Gateway SSL Scanner**

Helps you protect your network against attacks via the HTTPS protocol and prevents the disclosure of confidential corporate data, as well as infringements of Internet usage policies, thus ensuring that no one is illicitly sharing sensitive corporate materials.

---

## Importing licenses

The table below provides information on what happens when licenses are imported to versions 6.8.3 and 6.8.4 of McAfee Web Gateway under the new licensing model and in a few other scenarios:

<table>
<thead>
<tr>
<th>McAfee Web Gateway Version</th>
<th>Scenario</th>
<th>Implications</th>
</tr>
</thead>
</table>
| McAfee Web Gateway 6.8.3   | A Web Security Module license is imported. | • The anti-virus functions are enabled by default. These are the functions that are configured in the user interface under Anti Malware > Virus Scanning.  
• The caching functions are not available.  
• The Proactive Scanning functions are disabled by default, but the Proactive Scanning cache is enabled. |
| McAfee Web Gateway 6.8.3 with the Anti-Spam product included | An update to version 6.8.4 is performed. | • The anti-spam functions are still available.  
The old license is going to expire, but use of the anti-spam functions is still required.  
The license period must be extended under the old model. It must not be replaced by a licence under the new model because this will not cover any anti-spam functions. |
| McAfee Web Gateway 6.8.4   | A Web Security Module license is imported. | • The anti-virus functions are disabled by default.  
McAfee Web Gateway is run with an old license for the McAfee Anti-Virus engine and a Web Anti-Malware Module license is imported.  
• The anti-virus functions are enabled by default.  
• However, only the Secure Anti-Malware (SAM) engine is configured as anti-virus engine that has priority.  
A Web Security Module license is imported first and then a Web Anti-Malware Module license.  
• The anti-virus functions are disabled by default.  
• Only the McAfee Anti-Virus engine is configured as anti-virus engine that has priority.  
A Web Anti-Malware Module license is imported first and then a Web Security Module license.  
• The anti-virus functions are enabled by default.  
• No anti-virus engine is configured as having priority.  
The preconfigured AVOnly policy is applied.  
• The anti-virus functions are enabled all the time.  
• The Secure Anti-Malware engine is configured as anti-virus engine with the highest priority followed by the McAfee Anti-Virus engine. |
Home features

The features that are described in this chapter are accessible over the Home tab of the user interface:

These are basic features that are available in addition to the features of the individual products that can be run as parts of McAfee Web Gateway (formerly Webwasher®), such as system alerts, support contact, database feedback, and others.

Dashboard

The dashboard is invoked by clicking the corresponding button under Home. After invoking it, the number and quality of system alerts is displayed on the left side of the user interface area:

System Alerts

- 2 Red Alerts
- 3 Orange Alerts
- 2 Yellow Alerts

Clicking each of the alert lines takes you to the Overview tab, where the meaning of the alerts is explained and what to do about them, see Overview.

The tabs of the dashboard are described in the upcoming sections:

- Executive summary
- Traffic volume
- System
- McAfee Web Gateway

Before this is done, however, the following subsection provides some general information on the dashboard.
Handling the dashboard

The dashboard allows you to view summary information on a number of McAfee Web Gateway and system parameters at a glance. This information is in most cases displayed with regard to a particular time interval, such as the number of URLs that were filtered by McAfee Web Gateway over the last three hours.

If percentages were calculated for a group of related parameter values, they are shown by means of a pie chart on the left side of the corresponding tab section:

**Memory Utilization (Physical Memory)**

Average (last 1 Hour)

- Free
- Used

By hovering over the sections of the pie chart with the mouse cursor, you can display the individual percentages:

On the right side of a section, parameter values are shown as they developed in time, using either a line or a stacked mode:

Show last: 1 Hour

1.2GB
1012.3MB
759.2MB
306.1MB
253.1MB

More information about the values that are measured and displayed is provided in the upcoming sections.
The following activities can be performed for most of the dashboard values:

- **Selecting categories** — You can select the categories you want to have values displayed for with regard to a particular parameter.

To do this, just select or deselect the checkboxes next to the categories:

- **Good**
- **Blocked by AV Engine**
- **Blocked by Proactive**
- **Blocked by URL Filter**

In the above example, only the values (numbers in this case) of URLs that were “good” — passed all filtering — are selected for display, together with those that were blocked by the URL Filter, but omitting those that were blocked by an anti-virus engine or Proactive Scanning.

After selecting or deselecting a category, it is immediately displayed or removed from display.

The color of a category in the selection list is also used when the category is displayed in proportion to other categories by means of a pie chart.

Furthermore, this color is used to represent the category in stacked or line mode:

There is a limit to the display of some parameters. There may be values in more than six categories for these parameters, but only six categories and their values are shown at the same time.
By default, these are the categories with the top six values. You can, however, select other categories for display, using the drop-down lists, which are provided with the categories, but not more than six:

If you have made your own selection of categories, clicking **Select top 6 average values** will again display the six top value categories.

Since only the categories are shown that yielded the top six values or the categories you selected on your own, values that may have occurred in other categories are ignored here.

To get a representation of the total amount of values, you need to select **Others** as a category:

The values for five selected categories will then be shown, together with **Others**, which means that actually all categories and their values are covered.

- **Selecting a time interval** — You can select the time interval you want to view values for.

  Use the **Show last** drop-down list provided in the corresponding tab section to do this:

  The time scale and values displayed for the categories are immediately adapted according to the selected time interval.
The representation of values is influenced by the time interval you select. If this interval is no more than 6 Hours, each value shown in the sequence of values (for stacked or line mode) represents what was measured by McAfee Web Gateway during one minute.

For larger intervals, the values shown represent what was measured during ten minutes, or even longer periods of time. The maximum values provided by the measuring scale are modified accordingly.

The following table shows how the interval used for measuring values increases when larger time intervals are represented:

<table>
<thead>
<tr>
<th>Time interval represented</th>
<th>Time interval used for measuring values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 6 hours</td>
<td>1 minute</td>
</tr>
<tr>
<td>Up to 2 days</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Up to 2 weeks</td>
<td>1 hour</td>
</tr>
<tr>
<td>Up to 1 year</td>
<td>1 day</td>
</tr>
</tbody>
</table>

- **Selecting stacked or line mode**

You can have parameter values displayed in stacked or line mode:

- In line mode, lines are displayed to represent the development of values within a given time interval:

- In stacked mode, filled-out areas are displayed to represent the development of values within a given time interval, but with value areas "stacked" one on top of the other. This means that you are always shown sums of values in this mode:

For this reason, the value scale changes when switching from line to stacked mode since it takes more of a scale to display values in stacked than in line mode.
To select either stacked or line mode, select the corresponding radio button in a tab section:

- Stacked
- Line

The mode of display is immediately adapted according to what you selected.

**Executive summary**

The Executive Summary tab looks like this:

There are three sections on this tab:

- **URL Executive Summary**
- **Mail Executive Summary**
- **Number of Feedbacks sent**
**URL Executive Summary**
This section displays the number of URLs that were processed by the McAfee Web Gateway filters within a given time interval and either passed without restrictions or were blocked by one of these filters.

Values are shown for the following categories:

- **Good** — URLs that passed the McAfee Web Gateway filters without any restrictions.
- **Blocked by AV Engine** — URLs that were blocked by one of the anti-virus engines implemented within McAfee Web Gateway.
- **Blocked by Proactive** — URLs that were blocked due to the configuration of the Proactive Scanning Filter of McAfee Web Gateway.
- **Blocked by URL Filter** — URLs that were blocked due to the configuration of the URL Filter of McAfee Web Gateway.

**Mail Executive Summary**
This section displays the number of e-mails that were processed by the McAfee Web Gateway filters within a given time interval.

*Note:* The section is only displayed if McAfee Web Gateway is configured as an e-mail gateway. The corresponding option is enabled under **Proxies**, see also the *McAfee Web Gateway System Configuration Administration Guide*.

Values are shown for the following categories:

- **Malware** — E-mails that were found to contain malware.
- **Spam level high** — E-mails that were classified as high-level spam.
- **Spam level medium** — E-mails that were classified as medium-level spam.
- **Spam level low** — E-mails that were classified as low-level spam.

**Number ofFeedbacks Sent**
The **Number of Feedbacks Sent** section displays the number of feedbacks that were sent to McAfee Web Gateway by customers within a given time interval.

Customers can send these feedbacks using the link provided in the URL Filter Database Feedback section on the Feedback tab under Home > TrustedSource.

Values are shown for the following categories:

- **Malware** — Feedbacks submitting samples of malware.
- **False Positives** — Feedbacks concerning e-mails that were incorrectly marked as spam by McAfee Web Gateway.
- **False Negatives** — Feedbacks concerning spam e-mails that were not marked by McAfee Web Gateway as such.
- **URLs** — Feedbacks concerning URLs.
Traffic volume

The Traffic Volume tab looks like this:

There are two sections on this tab:

- Traffic Volume per Policy
- Traffic Volume per Protocol

Traffic Volume per Policy
This section displays the traffic volume (in bytes, see also the Prefix list at the end of this subsection) for the various policies that have been configured under McAfee Web Gateway. These may be the default policies, but also policies that you have set up yourself. Volumes for policies are displayed as they occurred within a given time interval.

Note: Not more than six volumes for different policies are shown at the same time. For information about how to have volumes shown, see Handling the dashboard.

Values for the following policies are shown by default:

- AVonly
- default
- Emergency
Prefix list
The list below shows the prefixes that are used for multiples of bytes, with byte values calculated in binary mode to measure and display, for example, traffic volumes. It also shows the use of these prefixes with regard to multiples of 10 to measure and display other values; for example, numbers of hits.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Byte symbol</th>
<th>Byte unit</th>
<th>Binary value</th>
<th>Decimal value</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>—</td>
<td>B</td>
<td>Byte</td>
<td>$2^0$</td>
<td>$10^0$</td>
</tr>
<tr>
<td>K</td>
<td>Kilo</td>
<td>KB</td>
<td>Kilobyte</td>
<td>$2^{10}$</td>
<td>$10^{10}$</td>
</tr>
<tr>
<td>M</td>
<td>Mega</td>
<td>MB</td>
<td>Megabyte</td>
<td>$2^{20}$</td>
<td>$10^{20}$</td>
</tr>
<tr>
<td>G</td>
<td>Giga</td>
<td>GB</td>
<td>Gigabyte</td>
<td>$2^{30}$</td>
<td>$10^{30}$</td>
</tr>
<tr>
<td>T</td>
<td>Tera</td>
<td>TB</td>
<td>Terabyte</td>
<td>$2^{40}$</td>
<td>$10^{40}$</td>
</tr>
<tr>
<td>P</td>
<td>Peta</td>
<td>PB</td>
<td>Petabyte</td>
<td>$2^{50}$</td>
<td>$10^{50}$</td>
</tr>
<tr>
<td>E</td>
<td>Exa</td>
<td>EB</td>
<td>Exabyte</td>
<td>$2^{60}$</td>
<td>$10^{60}$</td>
</tr>
<tr>
<td>Z</td>
<td>Zetta</td>
<td>ZB</td>
<td>Zettabyte</td>
<td>$2^{70}$</td>
<td>$10^{70}$</td>
</tr>
<tr>
<td>Y</td>
<td>Yotta</td>
<td>YB</td>
<td>Yottabyte</td>
<td>$2^{80}$</td>
<td>$10^{80}$</td>
</tr>
</tbody>
</table>

Traffic Volume per Protocol
This section displays the traffic volume (in bytes) that occurred on the connections used by McAfee Web Gateway under the different protocols within a given time interval.

Values are shown for the following protocols:
- HTTP
- HTTPS
- FTP
- Mail
System

The **System** tab is shown here in two parts because of its size. The upper part of the tab looks like this:

### Update Status

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>last update</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartFilter</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
<tr>
<td>Secure Anti-Malware</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
<tr>
<td>ETtrust</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
<tr>
<td>McAfee</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
<tr>
<td>Sophos</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
<tr>
<td>Spam Filter Rules</td>
<td>13748</td>
<td>Never updated</td>
</tr>
<tr>
<td>Certificate Revocation Lists</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
<tr>
<td>Proactive Scanning Database</td>
<td>Not applicable</td>
<td>Never updated</td>
</tr>
</tbody>
</table>

### Open Ports (McAfee Web Gateway listener)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port</th>
<th>Protocol</th>
<th>Service</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>all interfaces</td>
<td>9090</td>
<td>HTTP</td>
<td>Web Interface</td>
<td>listening</td>
</tr>
<tr>
<td>all interfaces</td>
<td>9093</td>
<td>HTTP</td>
<td>End User Requests</td>
<td>listening</td>
</tr>
<tr>
<td>all interfaces</td>
<td>9091</td>
<td>HTTPS</td>
<td>Secure Web Interface</td>
<td>listening</td>
</tr>
<tr>
<td>all interfaces</td>
<td>1344</td>
<td>ICAP</td>
<td>ICAP Server</td>
<td>listening</td>
</tr>
</tbody>
</table>

### CPU Utilization (all CPUs)

Average (last 1 Day)

- System
- Idle
- McAfee Web Gateway

### Memory Utilization (Physical Memory)

Average (last 1 Hour)

- Free
- Used
The lower part looks like this:

There are seven sections on this tab:

- **Update Status**
- **Open Ports**
- **CPU Utilization**
- **Memory Utilization**
- **Swap Utilization**
- **Filesystem Utilization (Free Capacity)**
- **Network Utilization**
**Update Status**
This section displays the status of several McAfee Web Gateway filtering features. These can be updated to ensure that the latest filtering rules, methods, signatures, and so on, are used by McAfee Web Gateway. The following information is displayed for each feature:

- **Feature** — Name of the feature
- **Version** — Version of the feature
- **Last Update** — Time when the feature was last updated

**Open Ports**
This section displays the various ports that are currently open, with McAfee Web Gateway listening for requests sent over these ports. The following information is displayed for each port:

- **Interface** — IP address of site communicating with McAfee Web Gateway over the port
- **Port** — Port number
- **Protocol** — The protocol under which communication is going on over the port
- **Service** — The service McAfee Web Gateway delivers over the port
- **Status** — The status McAfee Web Gateway has with regard to the port

**CPU Utilization**
This section shows to what extent the CPUs of the system McAfee Web Gateway is running on have been used within a given time interval. Values are shown for the following percentages:

- **System** — The percentage of the CPU utilization caused by the system
- **Idle** — The percentage of idle time
- **McAfee Web Gateway** — The percentage of the CPU utilization caused by McAfee Web Gateway

**Memory Utilization**
This section displays the percentages and absolute values (in bytes) of free and used physical memory of the system McAfee Web Gateway is running on within a given time interval. Values are shown for the following categories:

- **Free** — Amount of physical memory that was free
- **Used** — Amount of physical memory that was used

**Swap Utilization**
This section displays the percentages and absolute values (in bytes) of free and used swap memory of the system McAfee Web Gateway is running on within a given time interval. Values are shown for the following categories:

- **Free** — Amount of swap memory that was free
- **Used** — Amount of swap memory that was used
**Filesystem Utilization (Free Capacity)**
This section displays the percentages of used memory on the file systems where the various McAfee Web Gateway folders reside.
Memory values are shown as they occurred within a given time interval for the following folders:
- temp Folder
- log Folder
- mail Folder
- conf Folder
- info Folder

**Network Utilization**
This section displays the percentages and absolute values (in bytes) of network utilization for requests that were received or sent by McAfee Web Gateway over all its interfaces within a given time interval.
Values are shown for the following request categories:
- **Received** — Requests received over the network
- **Sent** — Requests sent over the network
McAfee Web Gateway

The McAfee Web Gateway tab is also shown here in two parts because of its size. The upper part looks like this:
The lower part looks like this:

There are seven sections on this tab:

- **Proxy Requests**
- **ICAP Server Requests**
- **Memory Utilization**
- **Number of Threads**
- **System Load**
- **Open Connections (System)**
- **Served Connections**
**Proxy Requests**
This section displays the number of requests per second sent to McAfee Web Gateway running as proxy server within a given time interval.

All the requests displayed here are grouped into one category, which includes requests sent to the McAfee Web Gateway proxy running under the HTTP or HTTPS protocol, as well as requests sent over the user interface that is provided for users of McAfee Web Gateway and accessed via port 9090.

**ICAP Server Requests**
This section displays the number of requests per second sent to McAfee Web Gateway running as ICAP server within a given time interval.

These requests fall into the following categories:
- **Options** — Requests sent to McAfee Web Gateway to provide information on the options applying to the ICAP communication
- **Profile** — Requests sent to McAfee Web Gateway to provide information on the profile used during the ICAP communication
- **REQMOD** — Requests sent to McAfee Web Gateway during ICAP communication handled in REQMOD mode
- **RESPMOD** — Requests sent to McAfee Web Gateway during ICAP communication handled in RESPMOD mode

**Memory Utilization**
This section displays the amount (in bytes) of memory used by McAfee Web Gateway and provided by the system McAfee Web Gateway is running on within a given time interval.

**Number of Threads**
This section displays the number of threads that were started by the McAfee Web Gateway core program, as well as by components that were loaded by McAfee Web Gateway within a given time interval.

After loading the library of the Sophos Anti-Virus engine, at least ten additional threads are started.

Numbers are displayed for the following kinds of threads:
- **Native** — Threads that were started by the McAfee Web Gateway core program
- **External** — Threads started by components that were loaded by the McAfee Web Gateway core program plus one thread for this main program

  **Note:** The core program thread is always shown, so the number of threads displayed here is at least 1, even if no threads were started externally.

**System Load**
This section shows the load for the system McAfee Web Gateway is running on within a given time interval. The complete system load is displayed here, not just the load caused by McAfee Web Gateway.

**Open Connections (System)**
This section displays the number of connections opened for communication under the TCP protocol for the system McAfee Web Gateway is running on within a given time interval.

All open connections are included here (with the exception of connections opened under version 6 of the TCP protocol), not just those opened by McAfee Web Gateway.

The number of open connections can also be displayed using the `netstat -at` command under Linux or the `netstat -a -p tcp` command under Windows.
**Served Connections**

This section displays the number of connections that are served by McAfee Web Gateway, which means that McAfee Web Gateway is listening for requests sent over these connections in order to provide services as required. This number is also displayed with regard to a given time interval.

The services provided by McAfee Web Gateway are also displayed, together with the ports used to provide them, in the **Open Ports** section of the **System** tab.

Internal services are not counted here. Internal and non-internal ICAP services can be viewed and configured on the **ICAP Services** tab under **Proxies > HTTP Proxy**.

The following are examples of the services that may be displayed:

- **End User Requests** — Connections served by McAfee Web Gateway to process requests sent by end users
- **FTP Proxy** — Connections served by McAfee Web Gateway while running as FTP proxy
- **HTTP(S) Proxy** — Connections served by McAfee Web Gateway while running as HTTP or HTTPS proxy
- **ICAP Server** — Connections served by McAfee Web Gateway while running as ICAP server
Overview

The **Overview** options are invoked by clicking the corresponding button under **Home**. They are described in the upcoming section:

- **Overview**

**Overview**

The **Overview** tab looks like this:

- **System Alerts** - Displays important system warnings and messages
  - At least one Anti Virus engine cannot be loaded. → Download new AV engine
  - The default root certificate is used by SSL Scanner. In order to avoid security problems → create your own certificate.
  - There has been no Anti Virus update check for at least 3 days. → Check Update Manager
  - There has been no URL Filter Database update check for at least 3 days. → Check Update Manager
  - There has been no Spam Filter Database update check for at least 3 days. → Check Update Manager
  - Email server for notification delivery is not defined. → Define server and sender.
  - Recipient for general email notifications is not set. → Enter email address.
  - Recipient for Virus email notifications is not set. → Enter email address.
  - Postmaster email address is not defined. → Enter email address.

- **System Summary** - Displays the latest system modifications and updates
  - System Settings: Admin  Fri May 08 13:05:24 2009
  - Anti Virus Engine and Signatures: Cannot load Secure Anti-Malware engine  Never updated
  - Cannot load CA ETrust engine
  - Cannot load McAfee engine
  - Cannot load Sophos engine
  - Certificate Revocation Lists: Database Number: 0  Never updated
  - Proactive Scanning Database: Database Number: 113  Sat Mar 21 21:05:08 2009

- **One-Click Lockdown** - Use single strict policy
  - [Activate emergency mode]

- **Run Wizard**
  - [Spam Filter Setup]

- **Version Information**
  - Version: 6.3.4 Beta 4
  - Build Number: 4739
  - Part Number: 91-09949750-A
  - Build Date: May 7 2009
  - Operating System: Windows
  - [Check for New Versions]
There are five sections on this tab:

- **System Alerts**
- **System Summary**
- **One-Click Lockdown**
- **Version Information**
- **Version Information**

**System Alerts**

This section displays alerts to make you aware of any problems concerning the system status. The function underlying these alerts is also known as "Security Configurator".

To the left of each alert text, a field in red, orange, or yellow color indicates the relative importance of the alert. To the right of each alert text, a link is displayed. Click this link to navigate to a tab where you can configure the relevant settings as a measure against the problem that caused the alert.

Note: An alert is repeated on tab or tabs dealing with the topic in question.

**System Summary**

This section displays information on the system status. Information is provided on the user who is currently logged in and on the anti-virus engines that are installed.

Furthermore, the last updates of the databases containing the rules for filtering URLs, viruses, and spam are displayed, as well as the version of the Certificate Revocation List.

Clicking the links that are provided here will take you to the corresponding Update Manager tabs, where you can configure and manually perform updates of the databases.

**One-Click Lockdown**

The One-Click Lockdown section looks like this:

![One-Click Lockdown](image)

Using this section, you can enable an emergency mode to apply a single strict policy overruling all other policies.

This may be useful in a situation when a new virus emerges. You may then want to replace all policies that were configured for different users and user groups by one single policy, which is rather strict and binding for all.

To enable the emergency mode:

- Click **Activate emergency mode**

  ![Activate emergency mode](image)

  This button is a toggle switch. After enabling the emergency mode, the inscription on it will read **Back to normal mode**.
To disable the emergency mode:

- Click **Back to normal mode**

When the emergency mode is enabled, there is also an alert in the **System Alerts** section of this tab to remind you it is enabled:

![Emergency profile used for all connections. Turn it off when not necessary.]

It is recommended that you turn off the emergency mode when it is no longer needed.

To select the policy that will be used under the emergency mode, go to the **Mapping Process** section on the **Web Mapping** tab under **User Management > Policy Management**.

The default policy to be applied under the emergency mode is a policy named **Emergency**. You may also retain this policy and its settings or modify them according to your requirements.

**Run Wizard**

This section provides a link to the **Spam Filter Setup** tab, which is located under **Configuration > Wizards**. Click this link to go to this tab and configure the e-mail gateway for protection against spam messages.

**Version Information**

This section displays information on the product version and also some related information, such as the current software build or the operating system McAfee Web Gateway is running on.

To see if there is a newer version of the software available, click **Check for New Versions**.
Support

The **Support** options are invoked by clicking the corresponding button under **Home**. They are described in the upcoming section:

- **Support**

Support

The **Support** tab looks like this:

For technical assistance, please contact support as described on our corporate website under [McAfee Technical Support](http://www.securecomputing.com/techsupport).

There is the following section on this tab:

- **Assistance**

Assistance

This section provides a link to contact the McAfee Technical Support team. Clicking this link takes you to the Welcome Page of this team.

Please read the information on this page and complete the activities described there to get the support you require.
The **TrustedSource** options are invoked by clicking the corresponding button under **Home**. They are described in the upcoming sections:

- **TrustedSource**
- **Malware Feedback Black List**
- **URL Feedback Black List**
- **Feedback**

**TrustedSource** tab looks like this:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam False Positives Feedback Queue</td>
<td>Allows to send feedback to McAfee to improve spam filter</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>SMTP queue to use:</td>
<td>FeedbackFalsePositives</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>Send interval in minutes:</td>
<td>220 (0 means no automatic send)</td>
<td></td>
</tr>
<tr>
<td>E-Mail Address:</td>
<td><a href="mailto:FalsePositivesFeedback@WillBeCaughtByWebwasher.com">FalsePositivesFeedback@WillBeCaughtByWebwasher.com</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam False Negatives Feedback Queue</td>
<td>Allows to send feedback to McAfee to improve spam filter</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>SMTP queue to use:</td>
<td>FeedbackFalseNegatives</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>Send interval in minutes:</td>
<td>200 (0 means no automatic send)</td>
<td></td>
</tr>
<tr>
<td>E-Mail Address:</td>
<td><a href="mailto:FalseNegativesFeedback@WillBeCaughtByWebwasher.com">FalseNegativesFeedback@WillBeCaughtByWebwasher.com</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Feedback Queue</td>
<td>Allows to send feedback to McAfee to improve malware filter</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>SMTP queue to use:</td>
<td>FeedbackMalware</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>Send interval in minutes:</td>
<td>45 (0 means no automatic send)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Feedback</td>
<td>Allows to send feedback about URLs to McAfee to improve URL filter</td>
<td>![Help Icon]</td>
</tr>
<tr>
<td>Send interval in minutes:</td>
<td>120</td>
<td></td>
</tr>
</tbody>
</table>

**Privacy Statement**

The following link describes the data that is collected and reported by the feedback system:

- [https://wpm.webwasher.com/download/webwasher/trustedsource_feedback.pdf](https://wpm.webwasher.com/download/webwasher/trustedsource_feedback.pdf)

There are five sections on this tab:

- **Spam False Positives Feedback Queue**
- **Spam False Negatives Feedback Queue**
- **Malware Feedback Queue**
- **URL Feedback**
- **Privacy Statement**
Spam False Positives Feedback Queue

The Spam False Positives Feedback Queue section looks like this:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP queue to use</td>
<td>FeedbackFalsePositives</td>
</tr>
<tr>
<td>Send interval in minutes</td>
<td>220 (0 means no automatic send)</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td><a href="mailto:FalsePositivesFeedback@WillBeCaughtByWebwasher.com">FalsePositivesFeedback@WillBeCaughtByWebwasher.com</a></td>
</tr>
</tbody>
</table>

Using this section, you can configure the sending of feedback in order to improve the spam filter. E-mails that were released from a queue after receiving a digest e-mail will be copied to the false positives queue and sent from there to McAfee.

This feature is not enabled by default. If you would like to help improve the spam filter, please select the checkbox next to the section heading. After specifying this setting and other settings in this section, click Apply Changes to make these settings effective.

Use the following items to configure the false positives feedback:

- **SMTP queue to use** — From this drop-down list, select an e-mail queue. After being released from another queue, e-mails will be copied to this queue and later be sent to McAfee.

  The queue should be used for no other purpose than that of collecting false positives since it will be cleared after e-mails have been sent off.

  To see the e-mails that are in this queue, click See Content of Queue next to the drop-down list.

- **Send interval in ... minutes** — In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse between sending e-mails.

  The default interval is 240 minutes. Entering 0 here means that no e-mails will be sent automatically.

  E-mails can be sent manually, however, using the Queue Management page, which is launched after clicking the See Content of Queue link next to the drop-down list. On this page, click Send All to SecureLabs now to send the e-mails.

- **E-mail address** — In this input field, enter an e-mail address. All e-mails received by McAfee Web Gateway containing this address will be moved to the queue specified above.

  The default address is FalseNegativesFeedback@WillBeCaughtBy-Webwasher.com.

Spam False Negatives Feedback Queue

The Spam False Negatives Feedback Queue section looks like this:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP queue to use</td>
<td>FeedbackFalseNegatives</td>
</tr>
<tr>
<td>Send interval in minutes</td>
<td>200 (0 means no automatic send)</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td><a href="mailto:FalseNegativesFeedback@WillBeCaughtByWebwasher.com">FalseNegativesFeedback@WillBeCaughtByWebwasher.com</a></td>
</tr>
</tbody>
</table>

Using this section, you can configure the sending of feedback in order to improve the spam filter.

You can send e-mails that have erroneously not been classified as spam to an address that is configured in this section. After e-mails with this address have been received in the inbound queue of your McAfee Web Gateway, they will be moved from there to the false negatives queue and later be sent to McAfee.

This feature is not enabled by default. If you would like to help improve the spam filter, please select the checkbox next to the section heading. After specifying this setting and other settings of this section, click Apply Changes to make these settings effective.
Use the following items to configure the false negatives feedback:

- **SMTP queue to use** — From this drop-down list, select an e-mail queue. After being received in the inbound queue, an e-mail with the address specified further below will be moved to this queue as false negative and later be sent to McAfee.

  The queue should be used for no other purpose than that of collecting false negatives since it will be cleared after e-mails have been sent off.

  To see the e-mails that are in this queue, click **See Content of Queue** next to the drop-down list.

- **Send interval in ... minutes** — In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse between sending e-mails.

  The default interval is **240** minutes. Entering **0** here means that no e-mails will be sent automatically.

  E-mails can be sent manually, however, using the **Queue Management** page, which is launched after clicking the **See Content of Queue** link next to the drop-down list. On this page, click **Send All to SecureLabs now** to send the e-mails.

- **E-mail address** — In this input field, enter an e-mail address. All e-mails received by McAfee Web Gateway containing this address will be moved to the queue specified above.

  The default address is **FalseNegativesFeedback@WillBeCaughtBy-Webwasher.com**.

**Malware Feedback Queue**

The **Malware Feedback Queue** section looks like this:

<table>
<thead>
<tr>
<th>Malware Feedback Queue</th>
<th>allows to send feedback to Webwasher to improve malware filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP queue to use:</td>
<td>FeedbackMalware ▼ ➔ See Content of Queue</td>
</tr>
<tr>
<td>Send interval in minutes:</td>
<td>45 (0 means no automatic send)</td>
</tr>
</tbody>
</table>

Using this section, you can configure the sending of feedback in order to improve the malware filter.

An e-mail that was classified as spam and contains an attachment where no virus was found, will be copied to the malware queue and later be sent to McAfee. Small downloads will also be copied to this queue if at least one of the anti-virus engines or the Proactive Scanning filter detected a virus, but not all engines came to the same result.

This feature is not enabled by default. If you would like to help improve the malware filter, please select the checkbox next to the section heading. After specifying this setting and other settings in this section, click **Apply Changes** to make these settings effective.

Use the following items to configure the malware feedback:

- **SMTP queue to use** — From this drop-down list, select an e-mail queue. E-mails and small downloads matching the criteria explained above will be moved to this queue as malware and later be sent to McAfee.

  The queue should be used for no other purpose than that of collecting malware since it will be cleared after e-mails and downloads have been sent off.

  To see the e-mails that are in this queue, click **See Content of Queue** next to the drop-down list.

- **Send interval in ... minutes** — In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse between sending e-mails.

  The default interval is **240** minutes. Entering **0** here means that no e-mails will be sent automatically.

  E-mails can be sent manually, however, using the **Queue Management** page, which is launched after clicking the **See Content of Queue** link next to the drop-down list. On this page, click **Send All to SecureLabs now** to send the e-mails.
**URL Feedback**

The **URL Feedback** section looks like this:

- **URL Feedback** - allows to send feedback about URLs to Webwasher to improve URL Filter

  Send interval in minutes: 120

Using this section, you can configure the sending of feedback in order to improve the URL Filter. URLs that have not yet been included and categorized in URL Filter Database, can be submitted to the URL Filter Database feedback service, using the link provided on the **Feedback** tab under **Home > TrustedSource**. The feedback is transmitted using an SSL-secured HTTPS connection.

The time interval for sending feedback is configured here.

This feature is not enabled by default. If you would like to help improve the URL filter, please select the checkbox next to the section heading. After specifying this setting and the setting for the send interval, click **Apply Changes** to make these settings effective.

**Note**: Enter all internal domains into the URL Feedback Black List, so URLs for these domains are not collected.

Use the following item to configure the URL feedback:

- **Send interval in ... minutes** — In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse until the next feedback is sent automatically.

  The minimum interval you can specify is 30 minutes. The default interval is 120 minutes.

**Privacy Statement**

The **Privacy Statement** section looks like this:

**Privacy Statement**

The following link describes the data that is collected and reported by the feedback

- https://vpm.webwasher.com/download/webwasher/trustedsource_feedback

It provides a link that enables you to read the Data Protection and Privacy Statement on the McAfee feedback system.
Malware Feedback Black List

The **Malware Feedback Black List** tab looks like this:

There is the following section on this tab:

- **Malware Feedback Media Type Black List**

Malware Feedback Media Type Black List

Using this section, you can add a media type to the Media Type Black List for malware feedback. Objects belonging to the media types on this list will not be entered in the malware feedback queue.

To add a media type to the black list, use the area labeled:

- **Select media type from catalog**

  Select the media type you want to have blacklisted from the drop-down list provided here.

  Furthermore, use the following items when adding a media type:

  - **Description** — Input in this field is optional. You may enter a description of the media type here.
  - **Add to Malware Feedback Media Type Black List** — After selecting a media type, click this button to add it to the list.

The Feedback Media Type Black List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking the appropriate arrow symbols.

To sort the list in ascending or descending order, click the symbol next to the **Media Type** or **Description** column heading.

To edit an entry, type the appropriate text in the input field of the **Description** column.
Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in the input field of the **Media Type** or **Description** column, or in both, and enter this using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.

**URL Feedback Black List**

The **URL Feedback Black List** tab looks like this:

There is the following section on this tab:

- **URL Feedback Black List**

  **URL Feedback Black List**

  Defines URLs (or domains) that should not be collected in URL feedback. URLs on this list, for example, internal URLs within your network, will not be entered in the URL feedback queue.

  To add a URL to the black list, use the area labeled:

  - **Add new URL**

    In the input field provided here, enter the URL you want to have blacklisted. Then click **Add to Black List**.

**URL Feedback Black List**

Using this section, you can add URLs to the black list for URL feedback. URLs on this list, for example, internal URLs within your network, will not be entered in the URL feedback queue.

To add a URL to the black list, use the area labeled:

- **Add new URL**

  In the input field provided here, enter the URL you want to have blacklisted. Then click **Add to Black List**.
The URL Feedback Black List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the **URL** column. Then click **Apply Changes** to make your settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in the input field provided here and enter it using the **Enter** key of your keyboard. The list will then display only entries matching the filter.
- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.
  
  To delete all entries, select the **Select all** checkbox and click this button.

**Feedback**

The **Feedback** tab looks like this:

<table>
<thead>
<tr>
<th>TrustedSource</th>
<th>Malware Feedback Black List</th>
<th>URL Feedback Black List</th>
<th>Feedback</th>
</tr>
</thead>
</table>

**Feedback E-Mail Address** — Enables you to send your comments to the Webwasher team.

McAfee values your feedback on the Webwasher products. If you have comments or suggestions concerning these products, you can use the following e-mail address to send e-mail messages to the Webwasher team:

features@securecomputing.com

**URL Filter Database Feedback** — Lets you submit incorrect or undetected URLs and checks the progress of previous submissions.

Go to [URL Filter Database feedback](#) service to submit URLs or view progress.

(NOTE: You have to provide your Webwasher Extranet account and password. The transmission is SSL-secured)

There are two sections on this tab:

- **Feedback E-Mail Address**
- **URL Filter Database Feedback**
Feedback E-Mail Address

The Feedback E-Mail Address section looks like this:

**Feedback E-Mail Address**  Enables you to send your comments to the Webwasher team.

McAfee values your feedback on the Webwasher products. If you have comments or suggestions concerning address to send e-mail messages to the Webwasher team:

+ features@securecomputing.com

Using this section, you can send feedback concerning the McAfee Web Gateway products to McAfee.
To send your feedback, click the features@securecomputing.com link. This will open a new e-mail message where you can type feedback and send to the e-mail address provided.

URL Filter Database Feedback

The URL Filter Database Feedback section looks like this:

**URL Filter Database Feedback**  Lets you submit incorrect or undeclassified URLs and checks the progress of previous.

Go to a URL Filter Database feedback service to submit URLs or view progress.
(Note: You have to provide your Webwasher Extranet account and password. The transmission is SSL-secured.)

Using this section, you can submit uncategorized or incorrectly categorized URLs to McAfee.
To submit URLs, click the URL Filter Database feedback link. This will launch the login page for accessing the Webwasher Extranet.
After successfully logging in there, a Welcome Page is displayed. On this page, click the option labeled Feedback system for URL Filter categorization. Then follow the instructions given on the URL Filter Feedback page.

Manuals

The Manuals options are invoked by clicking the corresponding button under Home. They are described in the upcoming sections:

- **Documentation on main products**
- **Documentation on special products**
- **Additional documentation**
Documentation on main products

The Documentation on Main Products tab looks like this:

<table>
<thead>
<tr>
<th>Documentation on Main Products</th>
<th>Documentation on Special Products</th>
<th>Additional Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Documents</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deployment Planning Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Installation Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Quick Configuration Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>System Configuration Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Advanced Configuration Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Upgrade Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td><strong>Product Documents</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL Filter User's Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Anti Malware User's Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Anti Virus User's Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>Anti Spam User's Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td>SSL Scanner User’s Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
<tr>
<td><strong>Reference Document</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference Guide</td>
<td>(→ PDF)</td>
<td></td>
</tr>
</tbody>
</table>

There are three sections on this tab:

- **General Documents**
- **Product Documents**
- **Reference Document**

**General Documents**
This section allows you to view user documentation on planning, installing and configuring McAfee Web Gateway in general.

To view any of the documents listed here, click PDF in the same line. This will open a .pdf format version of the document.

**Product Documents**
This section allows you to view user documentation on individual McAfee Web Gateway products.

To view any of the documents listed here, click PDF in the same line. This will open a .pdf format version of the document.

**Reference Document**
This section allows you to view the McAfee Web Gateway Reference Guide. Click PDF in the same line. This will open a .pdf format version of the document.
The **Documentation on Special Products** tab looks like this:

<table>
<thead>
<tr>
<th>Documentation on Main Products</th>
<th>Documentation on Special Products</th>
<th>Additional Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Reporter Documents</strong></td>
<td>Provide information about installing, configuring and operating the McAfee Web Gateway reporting tool.</td>
<td></td>
</tr>
<tr>
<td>Web Reporter Installation and Configuration Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>Web Reporter User's Guide for Reporting</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td><strong>Instant Message Filter Documents</strong></td>
<td>Provide information about installing, configuring and operating the McAfee Web Gateway Instant Messenger.</td>
<td></td>
</tr>
<tr>
<td>Instant Message Filter Installation Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>Instant Message Filter User's Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td><strong>Special Environment Documents</strong></td>
<td>Provide information about setting up McAfee Web Gateway or products running with it in a special environment.</td>
<td></td>
</tr>
<tr>
<td>Setting Up NetCache with ICAP</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>Setting Up Webwasher® on Microsoft ISA Server</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>Setting Up Webwasher® with Blue Coat™</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>NTML Agent Set-up Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>HSM Agent Set-up Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td><strong>Appliance Documents</strong></td>
<td>Provide information about the McAfee Web Gateway appliances.</td>
<td></td>
</tr>
<tr>
<td>Appliance Installation and Configuration Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
<tr>
<td>Appliance Upgrade Guide</td>
<td>[→ PDF]</td>
<td></td>
</tr>
</tbody>
</table>

There are four sections on this tab:

- **Web Reporter Documents**
- **Instant Message Filter Documents**
- **Special Environment Documents**
- **Appliance Documents**

**Web Reporter Documents**
The **Web Reporter Documents** section allows you to view user documentation on the McAfee Web Gateway reporting tool.

To view any of the documents listed here, click **PDF** in the same line. This will open a .pdf format version of the document.

**Note**: The reporting tool currently in use for the McAfee Web security products is Secure Web Reporter. For information on this tool, see the corresponding user documentation.

**Instant Message Filter Documents**
The **Instant Message Filter Documents** section allows you to view user documentation on a legacy McAfee Web Gateway instant message filtering tool.

To view any of the documents listed here, click **PDF** in the same line. This will open a .pdf format version of the document.
**Special Environment Documents**

The **Special Environment Documents** section allows you to view user documentation on setting up McAfee Web Gateway or products running with it in a special environment.

To view any of the documents listed here, click **PDF** in the same line. This will open a .pdf format version of the document.

**Appliance Documents**

The **Appliance Documents** section allows you to view user documentation on the McAfee Web Gateway appliances.

To view any of the documents listed here, click **PDF** in the same line. This will open a .pdf format version of the document.

**Additional documentation**

The **Additional Documentation** tab looks like this:

<table>
<thead>
<tr>
<th>Documentation on Main Products</th>
<th>Documentation on Special Products</th>
<th>Additional Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release Notes</strong></td>
<td>Provide the latest information about current releases of the McAfee Web Gateway products</td>
<td></td>
</tr>
<tr>
<td>Release Notes</td>
<td>(⇒ TXT)</td>
<td></td>
</tr>
</tbody>
</table>

There is the following section on this tab:

- **Release notes**

**Release notes**

This section allows you to view release notes and other documents containing the latest information on the McAfee Web Gateway products.

To view any of the documents listed here, click **TXT** in the same line. This will open a .txt format version of the document.
Preferences

The Preferences options are invoked by clicking the corresponding button under Home. They are described in the upcoming section:

- Preferences

Preferences

The Preferences tab looks like this:

There are three sections on this tab:

- Change Password
- View Options
- Access Permissions

Change Password

The Change Password section looks like this:

Using this section, you can change the password for access to McAfee Web Gateway.
After specifying the appropriate input here, click Apply Changes to make the new password effective.
Use the following input fields to change your password:

- **Current Password** — Enter the current password here.
- **Password** — Enter the new password here.
- **Retype password** — Enter the new password here a second time to confirm it.

**View Options**
The **View Options** section looks like this:

Using this section, you can configure what you would like the user interface to display or not.

If you are only interested in viewing and configuring settings for Web traffic, you can hide the e-mail related settings and vice versa. Furthermore, you can configure the change warner dialog and the configuration hash to be displayed or not.

After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following checkboxes to configure view options:

- **View web related settings** — Make sure this checkbox is selected if you want to view the Web related settings.
- **View web mail related settings** — Make sure this checkbox is selected if you want to view the e-mail related settings.
- **Show change warner dialog** — Make sure this checkbox is selected if you want the change warner dialog to appear whenever you are attempting to leave a tab without saving changed settings.
- **Show configuration hash** — Select this checkbox to have the configuration hash displayed at the top of the user interface area.

**Access Permissions**
The **Access Permissions** section looks like this:

Using this section, you can configure permissions to control access to McAfee Web Gateway.

While you are logged in as administrator, other administrators or other users in administrator roles, might also try to log in. You can allow their simultaneous access, restrict it to read-only or even deny it completely.

To what extent you are allowed to configure access permissions for other administrators, depends on your seniority level. This is measured by a value between 0 and 100. You can only configure permissions for administrators with seniority levels lower than your own.
On the other hand, you may find your right to access McAfee Web Gateway restricted or denied when trying to log in because an administrator with an equal or higher seniority level is currently logged in and has configured the corresponding settings.

So, if your seniority level is 80 and you have configured read-only access for other administrators while you are logged in, this will apply to all administrators with a seniority level of 80 or below.

If an administrator with a level of 60 logs in, a window will open providing access in read-only mode. At the same time, the number of sessions is displayed that are currently active, as well as the number of sessions where the seniority level is equal to or higher than that of the administrator who is trying to log in.

Furthermore, the number of sessions is displayed where this administrator is allowed to modify access permissions. In this case, there are no such sessions because someone with an equal or higher seniority level, such as you, has already configured the corresponding settings in a particular way.

This administrator now has the choice of logging in with read-only access or not.

On the other hand, if an administrator with a seniority level of 100 logs in, this administrator is entitled to modify what you configured since your seniority level is only 80. This modification will also apply to sessions where other administrators are already logged in.

The seniority level is configured on the Role Definition tab under User Management > Administrators. Click Edit Role Permissions to open a window, where you can configure a value for the seniority level.

After specifying the appropriate settings here, click Apply Changes to make them effective.

Use the following radio buttons to configure access permissions:

- **Allow simultaneous access** — Make sure this radio button is selected if you want to allow simultaneous access. Furthermore, specify what kind of simultaneous access should be allowed:
  - **Allow read/write access** — Make sure this radio button is selected if you want to allow read/write access.
  - **Allow read only access** — Select this radio button to allow read only access.
  - **Deny simultaneous access** — Select this radio button to deny simultaneous access.
License

The License options are invoked by clicking the corresponding button under Home. They are described in the upcoming sections:

- Information
- Notification

Information

The Information tab looks like this:

<table>
<thead>
<tr>
<th>License Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
</tr>
<tr>
<td>Number of Clients</td>
</tr>
<tr>
<td>Current Clients</td>
</tr>
<tr>
<td>Evaluation License</td>
</tr>
<tr>
<td>Customer number</td>
</tr>
<tr>
<td>Key number / System number</td>
</tr>
</tbody>
</table>

McAfee End User License Agreement

The installation and deployment of McAfee software products are exclusively governed by the terms as set forth in McAfee Standard Terms and Conditions. You can find the most recent version at:


Import License

[ ] I have read the - end user license agreement and accept it

Licensed Products

- URL Filter          | Included
- Anti Malware        | Included
- Anti Virus          | Included
- Anti Spam           | Included
- Content Protection  | Included
- SSL Scanner         | Included
- Content Reporter    | Included
- Instant Message Filter | Included


There are four sections on this tab:

- **License Information**
- **McAfee End User License Agreement**
- **Import License**
- **Licensed Products**

**License Information**
This section displays information regarding the licenses of the McAfee Web Gateway software. Information is provided on the company that purchased the license, the time interval during which the license is valid and other licensing issues.

**McAfee End User License Agreement**
This section allows you to view the most recent version of the end user license agreement. To view this version, click the link that is provided here.

**Import License**
The **Import License** section looks like this:

```
<table>
<thead>
<tr>
<th>Import License</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Browse]</td>
</tr>
<tr>
<td>![You have to accept the EULA]</td>
</tr>
<tr>
<td>![I have read the end user license agreement and accept it]</td>
</tr>
</tbody>
</table>
```

Using this section, you can import a license for the McAfee Web Gateway software.

To import a license, proceed as follows:

1. Click **Browse** and browse for the license file you want to import.
   Before you can import it, you will have to accept the end user license agreement. To read it, click **end user license agreement**.
2. If you accept the agreement, select the checkbox labeled **I have read the end user license agreement and accept it**. This will turn the button saying **You have to accept the EULA first** into one saying **Activate License**.
3. Click this button to import the license.

**Licensed Products**
This section displays the McAfee Web Gateway products and shows whether they are covered by the licenses you have acquired.

For information on the license models that currently exist for McAfee Gateway, see the **McAfee Web Gateway product licenses** section of the **Introduction**.
The Notification tab looks like this:

The Notification tab looks like this:

- **System Notifications** - Send notifications upon license status
  - Send notification upon license expiry
    - Recipient: [Field]
  - Send notification if number of licensed clients will soon be exceeded
    - Recipient from 'Send notification upon license expiry' will be used

Before sending system notifications you must configure the delivery options: Edit Notification Mail Server

Test Notification Settings: Send Test Messages

- **Too Many Clients** - writes system log messages if connections were refused due to heavy work load or license exhaustion
  - Enable message to be written to system log
    - Message text: %d generated %t by %w

There are two sections on this tab:
- **System Notifications**
- **Too Many Clients**

**System Notifications**
The System Notifications section looks like this:

Using this section, you can configure e-mail notifications on license issues. These will be sent to the e-mail address of the recipient you specify here.

After specifying the appropriate information, click **Apply Changes** to make your settings effective.
Use the following items to configure the system notifications:

- **Send notification upon license expiry** — Make sure the checkbox provided here is selected if you want to use this option, and enter the recipient of the notification in the **Recipient** input field.

- **Send notification if number of licensed clients will soon be exceeded** — Make sure the checkbox provided here is selected if you want to use this option.

The recipient of this notification will be the one entered in the **Recipient** input field above.

To configure the settings for the server used to process the notifications, click **Edit Notification Mail Server**. This will open a window where you can specify the appropriate settings:

![Notification Settings](image)

After specifying the settings, click **OK** to make them effective.

Furthermore, there is a button labeled **Send Test Messages** in this section. Click this button to test your settings.

**Too Many Clients**

The **Too Many Clients** section looks like this:

![Too Many Clients](image)

Using this section, you can configure messages to be written to the system log if connections were refused due to heavy work load or license exhaustion.

After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following items to configure log messages:

- **Enable message to be written to system log** — Select this checkbox if you want log messages to be written to the system log.

- **Message text** — In this input field, enter the message text. The default text is `%d (generated %t by %o)`.

  You can use the variable log file parameters appearing in the default text to set up your own message text. Furthermore, you can use an event name and a severity parameter.

  The following table lists these parameters and their meanings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>%e</td>
<td>Short name of the event that caused the log file message to be written</td>
</tr>
<tr>
<td>%d</td>
<td>Description of the event</td>
</tr>
<tr>
<td>%s</td>
<td>Severity of the event</td>
</tr>
<tr>
<td>%t</td>
<td>Local time and time zone of the host that generated the log file message</td>
</tr>
<tr>
<td>%o</td>
<td>FQDN name of the host</td>
</tr>
</tbody>
</table>
Common features

The features that are described in this chapter are accessible over the Common tab of the user interface:

These are filtering features that are available in addition to the features of the individual products that can be run as parts of McAfee Web Gateway (formerly Webwasher®), such as media type filters, the Document Inspector, the White List, and others.

Quick snapshot

The quick snapshot for the common filtering functions is invoked by clicking on the corresponding button under Common. It is described in the upcoming section:

• Quick snapshot
**Quick snapshot**

The **Quick Snapshot** tab looks like this:

![Quick Snapshot Tab](image)

### Media Types by Hits

<table>
<thead>
<tr>
<th>Mediatype</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>text/xml</td>
<td>26</td>
</tr>
<tr>
<td>text/plain</td>
<td></td>
</tr>
<tr>
<td>text/html</td>
<td>24</td>
</tr>
<tr>
<td>video/x-ms-wmvt</td>
<td>3</td>
</tr>
<tr>
<td>video/x-ms-asf</td>
<td>2</td>
</tr>
<tr>
<td>image/jpeg</td>
<td>2</td>
</tr>
<tr>
<td>image/gif</td>
<td>2</td>
</tr>
<tr>
<td>application/pkix-xml</td>
<td>1</td>
</tr>
</tbody>
</table>

### Media Types by Volume

<table>
<thead>
<tr>
<th>Mediatype</th>
<th>Bytes transferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>text/xml</td>
<td>70.1KB</td>
</tr>
<tr>
<td>text/html</td>
<td>32.5KB</td>
</tr>
<tr>
<td>video/x-ms-wmvt</td>
<td>5.6KB</td>
</tr>
<tr>
<td>text/plain</td>
<td>3.2KB</td>
</tr>
<tr>
<td>video/x-ms-asf</td>
<td>2.3KB</td>
</tr>
<tr>
<td>image/jpeg</td>
<td>2.3KB</td>
</tr>
<tr>
<td>image/gif</td>
<td>2.3KB</td>
</tr>
<tr>
<td>application/pkix-xml</td>
<td>0.04KB</td>
</tr>
</tbody>
</table>
There are four sections on this tab:

- **Frequent Media Types by Hits**
- **Frequent Media Types by Volume**
- **Media Types by Hits**
- **Media Types by Volume**

Before these are described, however, the following subsection provides some general information on the quick snapshot features.

**Handling the quick snapshot**

The quick snapshot features allow you to view summary information on several common filtering parameters at a glance.

For two of them, information is displayed with regard to a particular time interval, such as the number of media that were processed by the Media Type Filter over the last three hours, categorized, and grouped according to the media type.

Percentages are calculated for the individual categories, which are shown by means of a pie chart on the left side of the corresponding tab section.

On the right side of a section, parameter values are shown as they developed in time, using either a stacked or a line mode.

The pie chart and the representation in stacked or line mode are handled in the same way as on the McAfee Web Gateway dashboard.

You can:

- Select and deselect categories for display by selecting and deselecting the corresponding checkboxes:

  ![Checkbox examples]

  - text/html
  - text/plain
  - video/x-ms-wmv

- Select a time interval for display, using the **Show last** drop-down list:

  ![Show last dropdown]

  - 1 Hour

- Select stacked or line mode for display by checking the corresponding radio button:

  ![Radio buttons]

  - Stacked
  - Line

For a more detailed description of these activities, see the subsection labeled **Handling the dashboard** in the **Dashboard** section under **Home**.

There is, however, a property of the quick snapshot features that is not present on the dashboard tabs:

- **Resetting top value lists**

  For the **Media Types by Hits** and **Media Types by Volume** parameters, top value lists are displayed, using the length of bars to indicate the number of hits or the amount of bytes for various categories:

  ![Top value lists]

  - text/html: 32.6KB
  - video/x-ms-wmv: 5.6KB
  - text/plain: 3.2KB
  - video/x-ms-asf: 2.3KB
  - image/gif: 2.3KB
  - image/jpg: 2.3KB
You can choose to view the top 10, 25, and so on:

<table>
<thead>
<tr>
<th>Top 10</th>
</tr>
</thead>
</table>
| Top 10  
| Top 25  
| Top 50  
| Top 100 
| Top 200 
| Top 500 |

The top value lists can be reset with a reset button. After clicking this button, all values in a list are set to zero, so the measurement of values can start all over again.

A timestamp is displayed, indicating date and time of the last reset.

**Frequent Media Types by Hits**
The **Frequent Media Types by Hits** section displays the media types that were most often processed by the Media Type Filter within a given time interval.

**Frequent Media Types by Volume**
The **Frequent Media Types by Volume** section displays the media types that were processed by the Media Type Filter and consumed the greatest bandwidth volume (in bytes).

**Media Types by Hits**
The **Media Types by Hits** section displays a list of the top media types, showing the number of hits for each of them. Hit numbers are accumulated until the section is reset.

The following information is displayed for each media type:
- **Media type** — Name of the media type
- **Hits** — Number of times that this media type was processed by the Media Type Filter.

**Media Types by Volume**
The **Media Types by Volume** section displays a list of the top media types, according to the bandwidth (in bytes) consumed by each of them. Volumes are accumulated until the section is reset.

The following information is displayed for each media type:
- **Media type** — Name of the media type
- **Bytes transferred** — Number of bytes transferred for the media type.
Common
Media type filters

Media type filters

The Media Type Filters options are invoked by clicking on the corresponding button under Common.

If you want to enable any of these options, make sure the checkbox on this button is also selected. The checkbox is selected by default. After modifying the setting of this checkbox, click Apply Changes to make the modification effective.

These are policy-dependent options — they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled Policy, which is located above the Media Type Filters button:

- **Actions**
- **Media Type Black List**
- **Media Type White List**

Actions

The Actions tab looks like this:

<table>
<thead>
<tr>
<th>Actions</th>
<th>Media Type Black List</th>
<th>Media Type White List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Media Type Filter</strong></td>
<td>Manages the flow of media types for mail and Web downloads</td>
<td></td>
</tr>
<tr>
<td>Default action for unlisted media types</td>
<td>WEB Allow</td>
<td>MAIL Allow</td>
</tr>
<tr>
<td>Entry found in Media Type Black List</td>
<td>WEB Block</td>
<td>MAIL Replace and Quarantine</td>
</tr>
<tr>
<td>Entry found in Media Type White List</td>
<td>WEB Allow</td>
<td>MAIL Allow</td>
</tr>
<tr>
<td>Non-redistributable media types with magic bytes mismatch</td>
<td>WEB Block</td>
<td>MAIL Replace and Quarantine</td>
</tr>
<tr>
<td>Response without Content-Type header</td>
<td>WEB Allow</td>
<td>MAIL Allow</td>
</tr>
</tbody>
</table>

There are two sections on this tab:

- **Media Type Filter**
- **Web Upload Filter**
**Media Type Filter**

The **Media Type Filter** section looks like this:

<table>
<thead>
<tr>
<th>Media Type Filter</th>
<th>Action for Unlisted Media Types</th>
<th>Action for Media Type Black List</th>
<th>Action for Media Type White List</th>
<th>Action for Non-Rectifiable Media Types with Magic Bytes Mismatch</th>
<th>Action for Response Without Content-Type Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default action for unlisted media types</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
</tr>
<tr>
<td>Entry found in Media Type Black List</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
</tr>
<tr>
<td>Entry found in Media Type White List</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
</tr>
<tr>
<td>Non-Rectifiable Media Types with Magic Bytes Mismatch</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Block ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
</tr>
<tr>
<td>Response without Content-Type Header</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
<td><strong>WEB</strong> Allow ▼</td>
</tr>
</tbody>
</table>

Using this section, you can configure actions for the Media Type Filter. This filter manages the flow of incoming media types for HTTP and FTP downloads, as well as for SMTP.

A media (content) type is a general category of data content, such as an application, audio content, a text message, an image, a video stream, and so on. The media type tells the application that receives the data what kind of application is needed to process the content, for example, Real Audio is to play the audio content for a user.

Each of these media types also have subtypes, for example, the text media type has four subtypes: plain, rich text, enriched, and tab-separated values.

The actions that you configure here will be executed according to the result achieved by the Media Type Filter for a filtered object. You can also configure different actions for Web and e-mail traffic.

After specifying the appropriate settings here, click **Apply Changes** to make them effective.

Use the drop-down lists provided here to configure actions in the following way:

- **Default action for unlisted media types** — Select actions here that will be executed to a media type that is not listed in the Media Type White List or Black List.

- **Entry found in Media Type Black List** — Select actions here that will be executed for media types that are found in the Media Type Black List.

- **Entry found in Media Type White List** — Select actions here that will be executed for media types that are found in the Media Type White List.

- **Non-rectifiable media types with magic bytes mismatch** — Select actions here that will be executed when content types do not match their magic byte sequence.

  For example, a JPEG image declared as GIF file would be affected by a blocking action, even though each of these media types are acceptable.

- **Response without Content-Type header** — Select actions here that will be executed when media type information is contained in a response header.
Web Upload Filter

The Web Upload Filter section looks like this:

Using this section, you can configure actions for the Web Upload Filter. This filter protects corporate privacy and sensitive data by filtering what employees send out, such as FTP uploads or file attachments sent through common HTTP-based Web mail services, such as Hotmail or GMX.

You can limit the size that uploads may have or even forbid uploads of all HTTP and FTP files.

The actions that you configure here will be executed according to the result achieved by the Media Type Filter for a filtered object. You can also configure different actions for Web and e-mail traffic.

After specifying the appropriate settings here, click Apply Changes to make them effective.

Furthermore, you need to enable an option on the REQMOD Settings tab to use this filter. To do this, click REQMOD Settings provided at the bottom of this section. The option in question is Apply configured filters on uploaded and posted data.

Use the following items to configure the Web Upload Filter:

- **Maximal size of uploaded parameter ... kb** — In the input field provided here, enter a value to limit the size (in KB) of form data that is uploaded, such as sender and recipient information or text in an e-mail. For limiting the size of files that are uploaded, use the option below.

- **Maximal size of uploaded file ... kb** — In the input field provided here, enter a value to limit the size (in KB) of files that are uploaded. Note that this option can be used in addition to the uploaded parameter option.

- **Forbid uploads of all files (HTTP)** — Select this checkbox to forbid uploads of all HTTP files.

- **Forbid uploads of all files (FTP)** — Select this checkbox to forbid uploads of all FTP files.

- **Default action for unlisted media types** — Should the filter find a media type that is not currently listed in the Media Type White List or Black List, this is what will happen to it.

- **Entry found in Media Type Black List** — The actions configured here will be executed for media types that are found in the Media Type Black List.

- **Entry found in Media Type White List** — The actions configured here will be executed for media types that are found in the Media Type White List.

- **Content not validated by magic bytes** — The actions configured here will be executed when content types do not match their magic byte sequence.

  For example, a JPEG image declared as GIF file would be affected by a blocking action, even though each of these media types are acceptable.
Media Type Black List

The Media Type Black List tab looks like this:

<table>
<thead>
<tr>
<th>Actions</th>
<th>Media Type Black List</th>
<th>Media Type White List</th>
</tr>
</thead>
</table>

Media Type Black List - Defines media types that will be blocked
Select media type from catalog:
- application/aco

Description: [Enter description here]
- Ignore in Media Type Filter
- Ignore in Web Upload Filter

Add to Media Type Black List | Add to all policies

Found 1 entries with "*"
Number of entries per page: 10

<table>
<thead>
<tr>
<th>Select</th>
<th>Media Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter:</td>
<td>application/aco</td>
<td>[Enter description here]</td>
</tr>
<tr>
<td>Ignore in Media Type Filter</td>
<td>Ignore in Web Upload Filter</td>
<td></td>
</tr>
</tbody>
</table>

There is the following section on this tab:
- Media Type Black List

Media Type Black List

Using this section, you can add a media type to the Media Type Black List. Objects belonging to media types on this list will be blocked.

To add a media type to the list, use the area labeled:
- Service Name — In this input field, enter the service name.

Select the media type you want to have blacklisted from the drop-down list provided here.

Furthermore, use the following items when adding a media type:
- Description — Input in this field is optional. You may enter a description of the media type here.
- Ignore in Media Type Filter — If this option is enabled, the media type in question will be ignored when the Media Type Filter is applied to Web and e-mail downloads.
- Ignore in Web Upload Filter — If this option is enabled, the media type in question will be ignored when the Web Upload Filter is applied to outbound user-originating files via HTTP, HTTPS, or FTP.
- Add to Media Type Black List — After selecting a media type, click this button to add it to the list.

This addition will be valid only under the policy you are currently configuring. To add a media type to the black list for all policies, select the checkbox labeled Add to all policies before clicking on the button.
The Media Type Black List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click the symbol next to the **Media Type** or **Description** column heading.

To edit an entry, type the appropriate text in the input field of the **Description** column and enable or disable the **Ignore in media type filter** and **Ignore in media type filter** options. Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in the input field of the **Media Type** or **Description** column, or in both, and enter this using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.

### Media Type White List

The **Media Type White List** tab looks like this:

There is the following section on this tab:

- **Media Type White List**
Media Type White List
Using this section, you can add a media type to the Media Type White List. Objects belonging to the media types on this list will be allowed to pass through.

To add a media type to the list, use the area labeled:

- **Select media type from catalog** — Select the media type you want to include in the white list from the drop-down list provided here.

Furthermore, use the following items when adding a media type:

- **Description** — Input in this field is optional. You may enter a description of the media type here.

- **Ignore in Media Type Filter** — If this option is enabled, the media type in question will be ignored when the Media Type Filter is applied to Web and e-mail downloads.

- **Ignore in Web Upload Filter** — If this option is enabled, the media type in question will be ignored when the Web Upload Filter is applied to outbound user-originating files via HTTP, HTTPS, or FTP.

- **Add to Media Type White List** — After selecting a media type, click this button to add it to the list.

  This addition will be valid only under the policy you are currently configuring.

  To add a media type to the white list for all policies, select the checkbox labeled **Add to all policies** before clicking on the button.

The Media Type White List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click the symbol next to the **Media Type** or **Description** column heading.

To edit an entry, type the appropriate text in the input field of the **Description** column and enable or disable the **Ignore in media type filter** and **Ignore in media type filter** options. Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in the input field of the **Media Type** or **Description** column or in both and enter this using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.
The Document Inspector options are invoked by clicking on the corresponding button under Common. If you want to enable any of these options, make sure the checkbox on this button is also selected. The checkbox is selected by default.

After modifying the setting of this checkbox, click Apply Changes to make the modification effective. These are policy-dependent options — they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled Policy, which is located above the Media Type Filters button:

![Policy selection interface]

The options are described in the upcoming section:

- Document Inspector

### Document Inspector

The Document Inspector tab looks like this:

![Document Inspector interface]

- **Document Download Filter** - Filters inbound documents
  - Encrypted document found
  - WEB: Block
  - Apply Text Categorization on downloaded documents

- **Document Upload Filter** - Filters outbound user-originating documents
  - Encrypted document found
  - WEB: Allow

- **Document Mail Filter** - Filters documents attached to e-mails
  - Encrypted document found
  - ENML: Allow

- **Document Types** - Specifies which filters are to be applied to which file formats

- **General Options** - Specifies options that apply to all Document Filters
There are five sections on this tab:

- **Document Download Filter**
- **Document Upload Filter**
- **Document Mail Filter**
- **Document Types**
- **General Options**

### Document Download Filter

The **Document Download Filter** section looks like this:

Using this section, you can configure actions for inbound office documents that may enter your corporate network from the Web and are potentially malicious.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003, and all known versions of Adobe Portable Document Format (PDF).

Furthermore, they include the following open document formats: Generic XML, Microsoft OpenXML, Oasis Open Document Format, and the Simple Object Access Protocol (SOAP), which is an XML-based communications protocol for applications.

These documents may contain “active” content. Word, Excel, PowerPoint and Microsoft Open XML support ActiveX controls and macros, while PDF and the Oasis Open Document Format support embedded JavaScript.

This active content may be hostile rather than friendly, so for full protection against files that are embedded into Microsoft Office, PDF or open format documents, you should use the filter provided by the Document Inspector to inspect these documents and block malicious content from entering your corporate network. In addition to this filter, you can apply text categorization to these documents.

If you want to use this filter here, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following items to configure actions for office documents:

- **Encrypted document found** — From the drop-down list provided here, select an action. This action will be executed if the filter detects an inbound office document that is potentially malicious.

- **Apply Text Categorization** — Select the checkbox provided here, to apply text categorization actions to inbound office documents.

To view or modify the actions that are currently configured for these actions, click **Text Categorization** in the checkbox inscription. This will take you to the **Text Categorization** tab, where you have access to the corresponding settings.
**Document Upload Filter**

The **Document Upload Filter** section looks like this:

Using this section, you can configure actions for outbound user-originating office documents that are potentially malicious.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003, and all known versions of Adobe Portable Document Format (PDF).

Furthermore, they include the following open document formats: Generic XML, Microsoft OpenXML, Oasis Open Document Format, and the Simple Object Access Protocol (SOAP), which is an XML-based communications protocol for applications.

These documents may contain “active” content. Word, Excel, PowerPoint, and Microsoft Open XML support ActiveX controls and macros, while PDF and the Oasis Open Document Format support embedded JavaScript.

This active content may be hostile rather than friendly, so for full protection against files that are embedded in Microsoft Office, PDF, or open format documents, you should use the filter provided by the Document Inspector to inspect these documents and block malicious content from entering your corporate network.

If you want to use this filter here, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following drop-down list to configure actions for office documents:

- **Encrypted document found** — Select an action here. This action will be executed if the filter detects an inbound office document that is potentially malicious.

**Document Mail Filter**

The **Document Mail Filter** section looks like this:

Using this section, you can configure actions for office documents that are attached to e-mails, such as a .pdf format document.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003, and all known versions of Adobe Portable Document Format (PDF).

Furthermore, they include the following open document formats: Generic XML, Microsoft OpenXML, Oasis Open Document Format, and the Simple Object Access Protocol (SOAP), which is an XML-based communications protocol for applications.

These documents may contain “active” content. Word, Excel, PowerPoint, and Microsoft Open XML support ActiveX controls and macros, while PDF and the Oasis Open Document Format support embedded JavaScript.

This active content may be hostile rather than friendly, so for full protection against files that are embedded in Microsoft Office, PDF, or open format documents, you should use the filter provided by the Document Inspector to inspect these documents and block malicious content from entering your corporate network.

If you want to use this filter here, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After specifying the appropriate settings, click **Apply Changes** to make them effective.
Use the following items to configure actions for office documents:

- **Encrypted document found** — From the drop-down list provided here, select an action if the filter detects an office document attached to an e-mail that is potentially malicious.

**Document Types**

The **Document Types** section looks like this:

<table>
<thead>
<tr>
<th>Document Types</th>
<th>Microsoft® Word</th>
<th>Microsoft® Excel</th>
<th>Microsoft® PowerPoint</th>
<th>Adobe® PDF</th>
<th>Generic XML</th>
<th>Micros OpenXML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Filter</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Upload Filter</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Mail Filter</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Using this section, you can configure which of the filters that are accessible over the other sections of this tab should be applied to which document formats.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003, and all known versions of Adobe Portable Document Format (PDF).

Furthermore, they include the following open document formats: Generic XML, Microsoft OpenXML, Oasis Open Document Format, and the Simple Object Access Protocol (SOAP), which is an XML-based communications protocol for applications.

These documents may contain “active” content. Word, Excel, PowerPoint, and Microsoft Open XML support ActiveX controls and macros, while PDF and the Oasis Open Document Format support embedded JavaScript.

This active content may be hostile rather than friendly, so for full protection against files that are embedded in Microsoft Office, PDF, or open format documents, you should use the filter provided by the Document Inspector to inspect these documents and block malicious content from entering your corporate network.

By default, all filters are configured to apply to all formats.

After modifying these settings, click **Apply Changes** to make the modification effective.

**Note:** In order to use the filters for documents in Microsoft Open XML or Oasis Open Document Format, you need to enable the **Archive Handler.**

Use the following checkboxes to modify the assignment of filters to document formats:

- **Download Filter** — Select or deselect the checkboxes in this line to have the download filter apply to the corresponding document formats.

- **Upload Filter** — Select or deselect the checkboxes in this line to have the upload filter apply to the corresponding document formats.

- **Mail Filter** — Select or deselect the checkboxes in this line to have the mail filter apply to the corresponding document formats.
General Options

The General Options section looks like this:

Using this section, you can configure filtering conditions and actions for office documents that will apply to all the filters made accessible over the other sections of this tab.

You can configure different actions for documents in Web and e-mail traffic.

After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following items to configure filtering conditions and actions:

- **Word 95 document format not readable** — From the drop-down lists provided here, select actions for documents in Web and e-mail traffic.
  
  These are required because this format is not supported by the Document Inspector, which means the documents in question are unreadable for this filter.

- **Structured Storage document, like Visio or MSI, not readable** — From the drop-down lists provided here, select actions for documents in Web and e-mail traffic.

- **Office document not readable** — From the drop-down lists provided here, select actions for documents in Web and e-mail traffic.
  
  These actions will be executed for any type of office documents that are unreadable, maybe due to their encryption.

- **Library not loadable or failed** — From the drop-down lists provided here, select actions for documents in Web and e-mail traffic.
  
  These actions will be executed if the Document Inspector library could not be loaded.

Archive Handler

The Archive Handler options are invoked by clicking on the corresponding button under Common.

If you want to enable any of these options, make sure the checkbox on this button is also selected. The checkbox is selected by default.

After modifying the setting of this checkbox, click **Apply Changes** to make the modification effective.

These are policy-dependent options — they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the Media Type Filters button:

The options are described in the upcoming section:

- **Archive Handler**
Archive Handler

The Archive Handler tab looks like this:

There are two sections on this tab:

- Archive Handling
- Archive Handling Options

Archive Handling

The Archive Handling section looks like this:

Using this section, you can configure blocking and other actions for encrypted, corrupted, multi-part archives, archives containing mail bombs (an archive is a mail bomb if its content size exceeds the limit set by the user), and archives exceeding the maximum recursion level — how deep archives are nested within each other.

The size and recursion level limits are configured in the Archive Handling Options section, which is also provided on this tab.
If a virus is contained within an archive that is compressed, the virus cannot be detected and prevented from downloading.

The Archive Handler decompresses the members of an archive one-by-one, and passes them on to the virus scanner. When the archive member containing the virus is decompressed, virus scanner detects the virus, so the archive can be blocked.

You can configure different actions for archives in Web and e-mail traffic.

After selecting these actions from the drop-down lists provided here, click **Apply Changes** to make your settings effective.

### Archive Handling Options

The **Archive Handling Options** section looks like this:

```
<table>
<thead>
<tr>
<th>Archive Handling Options</th>
<th>Defines how to handle archives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of unpacked archive</td>
<td>750 MB</td>
</tr>
<tr>
<td>Maximum recursion level</td>
<td>24</td>
</tr>
</tbody>
</table>
```

Using this section, you can configure limits for archive sizes and recursion levels.

After specifying the appropriate settings click **Apply Changes** to make them effective.

Use the following input fields to configure limits for archives:

- **Maximum size of unpacked archive** — Enter the maximum size (in megabytes) here that should be allowed for an archive.

- **Maximum recursion level** — Enter the maximum number of recursion levels here that should be allowed for an archive.

### Generic Header Filter

The **Generic Header Filter** options are invoked by clicking the corresponding button under **Common**.

If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

These are policy-dependent options — they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **Media Type Filters** button:

```
| Policy: | default | Media Type Filters |
```

They are described in the upcoming section:

- **Generic Header Filter**
**Generic Header Filter**

The **Generic Header Filter** tab looks like this:

![Generic Header Filter Tab](image)

There is the following section on this tab:

- **Header Filter List**

**Header Filter List**

Using this section, you can configure rules for the Generic Header Filter to delete headers and header content, add customized headers, modify existing header content, and execute any pre-defined or customized action on appropriate filtering conditions.

Rules can be configured for Web traffic using the HTTP or HTTPS protocol, as well as for e-mail traffic.

For e-mail traffic, there are two options to choose from: SMTP and Mail. If SMTP is selected, the configured settings will operate on the content of internal McAfee Web Gateway headers, such as `X-WW-From`, `X-WW-To`, or `X-Client-IP`.

If Mail is selected, settings will operate on the content of standard e-mail headers such as `Subject`, `From` and `To`.

The filtering conditions for handling headers in this way are entered in the fields of this section. For an explanation of them, see the corresponding online help page.

On this page, examples are also provided for configuring rules with regard to HTTP and HTTPS communication, as well as information on tagged expressions, which may be used when setting up rules.

Furthermore, you will find a procedure there to set up a rule that creates a custom parameter, which can be used for accessing a header or parts of it. This may be needed in case you want to enter the header in a log file or display it in message text.
Generic Body Filter

The **Generic Body Filter** options are invoked by clicking on the corresponding button under **Common**. If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **Media Type Filters** button:

<table>
<thead>
<tr>
<th>Policy:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>☑</td>
</tr>
<tr>
<td>Media Type Filters</td>
<td>☑</td>
</tr>
</tbody>
</table>

They are described in the upcoming section:

- **Generic Body Filter**
Generic Body Filter

The **Generic Body Filter** tab looks like this:

![Generic Body Filter Tab](image)

There is the following section on this tab:

- **Body Filter List**

**Body Filter List**

Using this section, you can configure the Generic Body Filter blocking and other actions for Web and e-mail content according to keywords, regardless of the URL it originates from.

When configuring the filter, rules are set up in the following format:

- If the 2nd byte of a file has the value of n,
- and the 3rd byte does not have the value of n,
- and within the bytes 100 to 200 a string of n can be found,
- then ...
The Generic Body Filter also supports case-insensitive operands by using an uppercase I in front of a quoted operand.

For example, to block all HTML pages encoded as UTF-16 you can configure a rule like the following:

```
0-128 Contains I"<\00h\00t\00m\00l\00t\00m\00l" Or 0-128 Contains I"<\00h\00t\00m\00l\00t\00m\00l"
```

With this rule, the first expression blocks UTF-16LE, and the second blocks UTF-16BE.

The rules for filtering body content in this way and the actions that are executed when a rule matches are entered in the fields of this section. For more information, see the corresponding online help page.

---

**Advertising filters**

The Advertising Filters options are invoked by clicking on the corresponding button under Common.

If you want to enable any of these options, select the checkbox that is on this button. Then click Apply Changes to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled Policy, which is located above the Media Type Filters button:

```
<table>
<thead>
<tr>
<th>Policy:</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Type Filters</td>
<td>✓</td>
</tr>
</tbody>
</table>
```

They are described in the upcoming sections:

- **Settings**
- **Link Filter List**
- **Dimension Filter List**
## Advertising filters

### Settings

The **Settings** tab looks like this:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Link Filter List</th>
<th>Dimension Filter List</th>
</tr>
</thead>
</table>

- **Link Filter** - Screen content based on information from the URL
  - Disable built-in filter list
    - Objects to be filtered:
      - Images
      - Windows
      - Scripts
      - Layers
      - Frames
      - Embedded objects
      - Forms
      - Text links
      - Backgrounds

- **Dimension Filter** - Eliminates banner ads and objects by size
  - Objects to be filtered:
    - Images
    - Applets
    - Plug-ins
    - Ignore objects without specified dimensions
    - Filter objects that are located on the same server

- **Pop-Up Filter** - Eliminates script-initiated pop-up browser windows
  - Also disable manually opened windows

- **Script Filter** - Manages code that manipulates browsers and systems
  - Filter scripts that a Web page executes on loading
  - Filter scripts that a Web page executes on closing
  - Prevent supplementary modification of the address
  - Prevent modification of the browser's status bar

- **Animation Filter** - Manages and filters animated images
  - Animated images:
    - Show only the first picture of an animation
    - Repeat animation 1 time(s)
    - Remove all animated images

- **Advertising Filter Settings** - Define rules for filtered objects
  - Replace filtered objects with:
    - a transparent image
    - another image `C:\Programmes\Webwasher CSM\bin\files\image.png`
  - Do not filter objects located within:
    - the same path
    - the same domain
  - Do not reduce filtered frame size
There are six sections on this tab:

- **Link Filter**
- **Dimension Filter**
- **Popup Filter**
- **Script Filter**
- **Animation Filter**
- **Advertising Filter Settings**

**Link Filter**

The **Link Filter** section looks like this:

Using this section, you can configure the filtering of content based on information from the URL of an object and specify different types of content that you want to have filtered. URLs can be added for filtering to the built-in filter list or edited. The list can be accessed on the **Link Filter List** tab.

If you want to use this filter, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. All content types are also included in the filtering by default. After modifying any of these settings, click **Apply Changes** to make the modification effective.

Use the following checkboxes to configure the filtering of links:

- **Disable built-in filter list** — If this option is enabled, the built-in filter list is used.

  **Caution:** Disabling the built-in filter list will severely impair the efficiency of advertisement filtering. You should only do this in case you provide a filter list of your own that you want to work with.

- **Objects to be filtered** — Select or deselect the checkboxes provided here according to the content types you want the filter to apply.

  The meaning of the checkboxes is as follows:

  - **Images** — Enables or disables the filtering of images.
  
  - **Windows** — Enables or disables the filtering of windows that are commonly known as pop-ups.

  A pop-up is a display area, usually a small window, that suddenly pops up in the foreground of the visual interface.

  - **Scripts** — Enables or disables the filtering of Java scripts.

  These are used on Web sites to do such things as automatically changing a formatted date on a Web page, causing a linked-to page to appear in a pop-up window, causing text or a graphic image to change during a mouse rollover, and so on.

  - **Layers** — Enables or disables the filtering of layers.

  Web pages are often made up of positioning layers in HTML code, which may include a background as well as images or text added on top. Layers are designed to be used with JavaScript to create dynamic pages.
Common Advertising filters

- **Frames** — Enables or disables the filtering of frames.
  
  Frames are used for independent control of multiple sections on a Web page. This is achieved by building each section as a separate HTML file and using one "master" HTML file to handle all sections.

  When a user requests a Web page that uses frames, the address requested is usually that of the master file.

- **Embedded Objects** — Enables or disables the filtering of embedded objects.
  
  Embedded objects are objects such as images, videos, Java applets that are created within another application and embedded into a document.

- **Forms** — Enables or disables the filtering of forms.

- **Text links** — Enables or disables the filtering of text links.
  
  A text link is the grouping of linked text that, when clicked on, takes you to another page either within the same Web site, or to an entirely different Web server.

  It will often open up another browser window when clicked on.

- **Backgrounds** — Enables or disables the filtering of background images.
  
  This option only removes advertising backgrounds, but not all background images in general.

**Dimension Filter**

The **Dimension Filter** section looks like this:

Using this section, you can configure a filter to eliminate banner ads and objects based on their size.

To add dimensions to the Dimension Filter List go to the **Dimension Filter List** tab.

If you want to use this filter, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following checkboxes to configure dimension filtering:

- **Objects to be filtered** — Select or deselect the checkboxes provided here according to the content types you want the filter to apply to.

  Their meaning is as follows:

  - **Images** — Enables or disables the filtering of images.
  
  - **Applets** — Enables or disables the filtering of Java applets.
    
    These are small programs accompanying a Web page that is sent to a user. Java applets are able to perform interactive animations, instant calculations and conversions, and so on, without having to send a user request back to the server.

  - **Plug-ins** — Enables or disables the filtering of plug-ins.
    
    These are programs that can easily be installed and used as part of your Web browser.
Common Advertising filters

- **Ignore objects without specified dimensions** — If this option is enabled, objects that have their dimensions not specified will be ignored.
- **Filter objects that are located on the same server** — If this option is enabled, objects will also be filtered if they are located on the same server. By default, such objects will go unfiltered.

**Popup Filter**
The **Popup Filter** section looks like this:

- **Pop-Up Filter** - Eliminates script-initiated pop-up browser windows
- Also disable manually opened windows

Using this section, you can configure a filter to eliminate script-initiated pop-up browser windows. You can also disable manually opened windows to ensure that pop-up windows remain closed.

If you want to use this filter, select the checkbox next to the section heading. After specifying this setting, you may also specify the additional setting provided here. Then click **Apply Changes** to make your settings effective.

Use the following checkbox to configure the additional setting:
- **Also disable manually opened windows** — If this option is enabled, pop-ups will not be opened even if the user clicks on the corresponding link.

**Script Filter**
The **Script Filter** section looks like this:

- **Script Filter** - Manages code that manipulates browsers and systems
- Filter scripts that a Web page executes on loading
- Filter scripts that a Web page executes on closing
- Prevent supplementary modification of the address
- Prevent modification of the browser's status bar

Using this section, you can configure a filter to manage the code that manipulates browsers and systems. If you want to use this filter, select the checkbox next to the section heading. After specifying this setting or any other setting in this section, click **Apply Changes** to make these settings effective.

Use the following checkboxes to configure script filtering:
- **Filter scripts that a Web page executes on loading** — If this option is enabled, the filter will suppress scripts that are started automatically when a Web page is loaded. The option is enabled by default.
- **Filter scripts that a Web page executes on closing** — If this option is enabled, the filter will suppress scripts that are started automatically when a Web page is closed. The option is enabled by default.
- **Prevent supplementary modification of the address** — If this option is enabled, the filter will suppress special JavaScript functions that modify the IP address—JavaScript functions that automatically transfer you from one Web page to another.
- **Prevent modification of the browser's status bar** — If this option is enabled, the filter will prevent the status bar of the browser from being modified by a Web page, such as scrolling text.
**Animation Filter**

The Animation Filter section looks like this:

- **Animation Filter** - Manages and filters animated images
  - Animated images:
    - Show only the first picture of an animation
    - Repeat animation \( n \) time(s)
    - Remove all animated images

Using this section, you can configure a filter to detect animated images. Animations will either be filtered completely or restricted in their execution.

If you want to use this filter, select the checkbox next to the section heading. After specifying this setting or any other setting in this section, click **Apply Changes** to make these settings effective.

Use the following radio buttons to configure animation filtering:

- **Animated images** — Use the radio buttons provided here according to the measures you want the filter to take against animations:
  - **Show only the first picture of an animation** — Make sure this button is checked to terminate an animation after showing the first picture. This option is enabled by default.
  - **Repeat animation ... time(s)** — Select this button to limit repetition of the animation.
    - In the input field provided here enter the number of times you want an animation to repeat itself.
  - **Remove all animated images** — Select this button to remove animation completely.

**Advertising Filter Settings**

The Advertising Filter Settings section looks like this:

- **Advertising Filter Settings** - Define rules for filtered objects
  - Replace filtered objects with:
    - a transparent image
  - another image: C:\Programmes\Webwasher\CSD\bin\files\image
  - Do not filter objects located within:
    - the same path
    - the same domain
  - Do not reduce filtered frame size

Using this section, you can configure settings that will apply to all the filters on this tab.

After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following checkboxes and radio buttons to configure these settings:

- **Replace filtered objects with** — Select this checkbox if you want to have filtered objects replaced with something.
  - Then select the radio buttons below to specify with what they should be replaced:
    - a transparent image — Enable this option to replace an animated image with a transparent image.
Common Advertising filters

- **another image** — Make sure this option is enabled if you want to replace an animated image with another image.
  
  In the input field provided here, enter the path and name of the image you want to use.
  
  The option is enabled by default. Likewise, a default image is configured to replace animations.

- **Do not filter objects located within** — Select this checkbox if you want to exclude objects from filtering that are within the same path or domain.
  
  Then select the radio buttons below to further specify the exclusion:

  - **the same path** — Enable this option to exclude objects within the same place from filtering.
  
  - **the same domain** — Enable this option to exclude objects within the same domain from filtering.

- **Do not reduce filtered frame size** — Select this checkbox to prevent filtered frame sizes from being reduced.

**Link Filter List**

The **Link Filter List** tab looks like this:

![Link Filter List Tab](image)

There is the following section on this tab:

- **Link Filter List**
**Link Filter List**

Using this section, you can add URLs to the Link Filter List and edit them.

To do this, use the area labeled:

- **Add new URL** — Select **String** or **International Domain Name** from the first of the drop-down lists provided here.

  In the input field next to it, enter a string to specify the object using shell expressions.

  Select **International Domain Name** if you want to enter non-ASCII characters and the string should be used for the domain part of an URL.

  In some countries like Germany, Sweden, or Japan, domain names with non-ASCII characters are allowed. The IDNA (International Domain Names in Applications) standard describes how a Web browser should convert such a domain name into pure ASCII notation used, such as by DNS.

  McAfee Web Gateway uses the pure ASCII notation as well, therefore all IDN strings must be converted. This is done automatically when you select **International Domain Name** and enter a string with non-ASCII characters.

  **Note:** You cannot use shell expressions with IDN strings.

Furthermore, use the following items when adding a new entry to the list:

- **deactivate** — Enable this option to insert a new URL in the list that will not yet be used for filtering.

- **do not filter** — Enable this option to exclude the URL you entered above from filtering.

- **Add to Link Filter List** — After specifying the information for a URL, click this button to add it to the list.

  This addition will be valid only under the policy you are currently configuring. To add a URL to the list for all policies, select the checkbox labeled **Add to all policies** before clicking the button.

  If a URL or shell expression that was configured under another policy is already in the list, the setting of the **Add to all policies** checkbox will have no effect.

The Link Filter List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click the symbol next to the **URL** column heading.

To edit an entry, type the appropriate text in the corresponding input field and select or deselect the **deactivate** and **do not filter** checkboxes in the same line. Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in this input field and enter it using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.
Common

Advertising filters

**Dimension Filter List**

The **Dimension Filter List** tab looks like this:

There is this the following section on this tab:

- **Dimension Filter List**

**Dimension Filter List**

Using this section, you can add dimension settings to the Dimension Filter List and edit them. These can be used for filtering images, applets, or plug-ins.

To do this, use the area labeled:

- **Add new dimension** — In the input field provided here, enter a pair of pixel values to specify the height and width of an object that should be filtered.

Furthermore, use the following item when adding dimension settings to the list:

- **deactivate** — If this option is enabled the corresponding dimension settings will be added to the list, but not yet used for filtering.

- **Add to Dimension Filter List** — After specifying the dimensions settings in the way described above, click this button to add them to the list.

This addition will be valid only under the policy you are currently configuring. To add dimensions to the list for all policies, select **Add to all policies** checkbox before clicking the button.

If dimension settings that were configured under another policy are already in the list, the setting of the **Add to all policies** checkbox will have no effect.
The Dimension Filter List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate pixel values in the corresponding input field and select or deselect the **deactivate** checkbox in the same line. Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in this input field and enter it using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.

### Privacy filters

The **Privacy Filters** options are invoked by clicking on the corresponding button under **Common**.

If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **Media Type Filters** button:

<table>
<thead>
<tr>
<th>Policy:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>✔</td>
</tr>
</tbody>
</table>

| Media Type Filters | ✔ |

They are described in the upcoming sections:

- **Settings**
- **Cookie Filter List**
Settings

The Settings tab looks like this:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Cookie Filter List</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Web Bug Filter - Eliminates mini-images used to track navigation Also applies using same technique in HTML mails</td>
<td></td>
</tr>
</tbody>
</table>
| ✔ Referer Filter - Removes strings that report the last page visited  
  Remove referer:  
  ○ always  
  ○ if the domain or the path is different  
  ○ if the domain is different |
| ✔ Prefix Filter - Removes URL prefixes used to track user behavior  
| ✔ Cookie Filter - Controls passing of cookies to and from Web servers  
  Disable built-in filter list  
  Neutral cookies expire after:  
  ○ a time period of 24 h, 0 min  
  ○ finishing the browser session  
  Cookies not found in the Cookie Filter List are:  
  ○ good  
  ○ neutral  
  ○ bad |

There are four sections on this tab:

- Web Bug Filter
- Referer Filter
- Prefix Filter
- Cookie Filter

Web Bug Filter

The Web Bug Filter section looks like this:

| Web Bug Filter - Eliminates mini-images used to track navigation  
  Also applies using same technique in HTML mails |

Using this section, you can configure a filter to eliminate Web bugs. These are also known as clear GIFs or Web beacons. They are usually 1 pixel x 1 pixel mini-images in size and are used to track user navigation behavior on Web sites and in e-mail to see if an e-mail was opened by the recipient.

The filter is also applied to the same technique used in HTML messages.

If you want to use this filter, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After modifying this setting, click Apply Changes to make the modification effective.
Referer Filter

The **Referer Filter** section looks like this:

![Referer Filter](image)

Using this section, you can configure a filter to remove referer strings that report the last page visited by a user.

If you want to use this filter, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After modifying this setting or any other setting in this section, click **Apply Changes** to make the modification effective.

To configure the filtering of referer strings, use the radio buttons of the area labeled:

- **Remove referer** — Select or deselect one of these three radio buttons as needed:
  - **always** — If this option is enabled a referer is always removed regardless of where the user in question came from.
  - **if the domain or the path is different** — If this option is enabled a referer is removed if the user came from a different path or URL.
    
    It leaves the referer unaffected if you the user moves through the same or subsequent path.
    
    This option may be enabled if user movement should be hidden, but there are services that rely on a referer to work properly.
  - **if the domain is different** — If this option is enabled a referer is removed in case the user came from a different Web site.
    
    It leaves the referer unaffected if the user moves through the same Web site. This allows the Web master to track user movement through this Web site. The information may be useful for adjusting or optimizing the navigational structure of the site.
    
    As well, some services such as online banking may need a referer to work properly.

Prefix Filter

The **Prefix Filter** section looks like this:

![Prefix Filter](image)

Using this section, you can configure a filter to remove all prefixes from URLs that are used by some sites to track user behavior.

If you want to use this filter, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After modifying this setting, click **Apply Changes** to make the modification effective.
**Cookie Filter**

The **Cookie Filter** section looks like this:

![Image of the Cookie Filter section]

Using this section, you can configure a filter to block bad cookies. You can set the life span for neutral cookies or let them expire after finishing the browser session.

The Cookie Filter controls the data stream between users and the Web in both directions, a requirement for efficient filtering. Transmitted cookies coming in on the Web server, in addition to those from the browser, are controlled by McAfee Web Gateway.

The distinction between the good, and thus necessary, cookies, and the bad cookies that invade privacy is carried out by McAfee Web Gateway using an algorithm and the built-in filter list depending on the URL of a cookie. To add and edit cookies on this list, go to the **Cookie Filter List** tab.

If you want to use this filter, make sure the checkbox next to the section heading is selected. The checkbox is selected by default. After modifying any of these settings, click **Apply Changes** to make the modification effective.

Use the following items to configure cookie filtering:

- **Disable built-in filter list** — If this option is enabled the built-in filter list is used. The option is disabled by default.

- **Neutral cookies expire after** — Use the radio buttons and input fields provided here in the following way:
  - **a time period of ... h ... min** — Make sure this radio button is checked if you want to configure a life span for neutral cookies. The radio button is checked by default.
    - Enter the appropriate time periods (in hours and minutes) in the input fields provided here. The default value is 24 hours.
  - **finishing the browser session** — Select this radio button to let neutral cookies expire when sessions are ended.
    - A pop-up is a display area, usually a small window, that suddenly pops up in the foreground of the visual interface.

- **Cookies not found in the filter list are** — Use the radio buttons provided to configure a default classification for cookies:
  - **good** — Select this radio button to classify unknown cookies as good.
  - **neutral** — Select this radio button to classify unknown cookies as neutral.
    - **Note:** Unknown cookies are classified so by default.
  - **bad** — Select this radio button to classify unknown cookies as bad.
Cookie Filter List

The **Cookie Filter List** tab looks like this:

There is the following section on this tab:

- **Cookie Filter List**

**Cookie Filter List**

Using this section, you can add entries to the Cookie Filter List and edit them. Shell expressions in this list will be compared to the domain where the cookie was sent from or will be sent to, in order to determine whether the cookie is good, neutral, or bad.

Good cookies can pass, bad cookies are filtered out, and neutral cookies will vanish after the configured life span.

To add a cookie to the list, use the area labeled:

- **Add new cookie** — In the input field provided here enter the cookie.

  Then classify it by checking one of these three radio buttons:

  - **good** — **neutral** — **bad** — The **neutral** button is checked by default.

  - **Add to Cookie Filter List** — After specifying a cookie and classifying it, click this button to add it to the list.

  This addition will be valid only under the policy you are currently configuring. To add a cookie to the list for all policies, select the checkbox labeled **Add to all policies** before clicking the button.

  If a cookie that was configured under another policy is already in the list, the setting of the **Add to all policies** checkbox will have no effect.
The Cookie Filter List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the cookie, and select or deselect the **good**, **neutral**, or **bad** button in the same line. Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in this input field and enter it using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

To delete all entries, select the **Select all** checkbox and click this button.

---

**Text categorization**

The **Text Categorization** options are invoked by clicking on the corresponding button under **Common**.

If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **Media Type Filters** button:

![Policy](image)

They are described in the upcoming sections:

- **Settings**
- **Categorization List**
Settings

The Settings tab looks like this:

There is the following section on this tab:

- **Text Categorization**

**Text Categorization**

Using the text categorization filter you can specify single keywords and combinations of words and filter office documents and e-mail attachments containing these words.

In this section, you configure the actions that should be taken whenever the text categorization filter matches. You can configure different actions for particular categories of documents. Furthermore, you can configure different actions for Web and e-mail traffic.

A confidential category is provided here for a start. Apart from this, you can configure actions for up to six categories of your own.

The rules for the keywords and combinations that should be filtered are configured and listed on the Categorization List tab.

If you want to configure actions for text categorization, select them from the appropriate drop-down lists. Then click **Apply Changes** to make your settings effective.

Select actions from the following lists:

- **Confidential** — Select actions for documents falling into the confidential category here.

- **User-Defined, User Defined 1, ...** — Select actions for documents falling into any of your own categories here.
**Text Categorization List**

The **Text Categorization List** tab looks like this:

There is the following section on this tab:

- **Text Categorization List**

**Text Categorization List**

Using the text categorization filter you can specify single keywords and combinations of words and filter office documents and e-mail attachments containing these words.

In this section, you can configure rules for the keywords and combinations of keywords that should be filtered and add them to the Text Categorization List.

To add a text categorization rule to the list, use the area labeled:

- **Add rule** — Use the following items to configure a rule and add it to the list:
  
  - **[term 1] AND [term 2] AND NOT [term 3]** — Make sure the radio button in this line is checked if you want to configure a rule according to this method, which is one of two provided here.
    
    This method uses Boolean logic to determine the placement of words in an office document or e-mail message. It is enabled by default.
    
    In the input fields, enter the words or word combinations you want to filter, such as Bahamas, Maldives, work to set up a rule like the following:
    
    Bahamas AND Maldives AND NOT work
    
  - **[term 1] more than [term 2] times per [term 3] words** — Select the radio button in this line to configure a rule according to the second method provided here.
  
    It is based on counting how often a particular word or combination appears in the text body of an office document or an e-mail message.
In the input fields, enter the word or word combination you want to filter, such as `money, 3, 10` to set up a rule like the following:

`money more than 3 times per 10 words`

- **Select one or more categories to apply to the above rule** — From the drop-down lists provided here select one or more categories.

The rule configured above will be applied within these categories.

- **Create Rule** — After setting up a text categorization rule, click this button to add it to the list.

This addition will be valid only under the policy you are currently configuring. To add a rule to the list for all policies, select the checkbox labeled **Add to all policies** before clicking on the button.

The Text Categorization List is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the `Enter` key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the rule. Enable or disable a rule by selecting or deselecting the **Deactivate** checkbox in the corresponding line.

Then click **Apply Changes** to make these settings effective. You can edit more than one list entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter expression in this input field and enter it using the `Enter` key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

To delete all entries, select the **Select all** checkbox and click this button.

### HTTP Method Filter List

The **HTTP Method Filter List** options are invoked by clicking on the corresponding button under **Common**. If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **Media Type Filters** button:

<table>
<thead>
<tr>
<th>Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
</tr>
<tr>
<td>Media Type Filters</td>
</tr>
</tbody>
</table>

The options are described in the upcoming section:

- **HTTP Method Filter List**
HTTP Method Filter List

The **HTTP Method Filter List** tab looks like this:

There is the following section on this tab:

- **HTTP Method Filter List**

**HTTP Method Filter List**

Using this section, you can configure rules for assigning actions to particular HTTP methods that occur in user requests and add these rules to a list. The rules may also include a categorization of the method and specify the URL it is applied to.

For example, you could set up a rule that categorizes the GET method when applied to a particular URL as **Entertainment** and blocks the corresponding request.

To add a rule to the list, use the area labeled:

- **Add rule**

Use the following items to configure the rule:

- **Method** — From this drop-down list, select the HTTP method you want to configure a rule for.

- **URL** — In this input field, enter the URL that is requested when the HTTP method is used. Input in this field is optional.

- **Category** — From this drop-down list, select a URL filtering category you want to assign to the HTTP method. Setting this category is also optional.

- **Action** — From this drop-down list, select the action you want to have executed if the rule matches.

- **Continue** — If this checkbox is selected, McAfee Web Gateway will look for further matches after the rule matched for the first time. Otherwise, filtering activities will be stopped after the first match.

- **Description** — Enter a description of the rule here. Input in this field is optional.
- **Add to HTTP Method Filter List** — After specifying the appropriate information in the fields above, click this button to add the rule to the list.

  The rule will be valid only under the policy you are currently configuring. To add a rule to the list that is valid for all policies, select the checkbox labeled **Add to all policies** before clicking on the button.

The HTTP Method Filter List is displayed at the bottom of the section. To display only a particular number of list entries at a time, type this number in the input field labeled **Number** of entries per page and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the **URL** or **Description** column, or in both, select the appropriate method, category, and action from the drop-down lists, and enable or disable the **Continue** option.

Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filtering term in the input field of the **URL** or **Description** column, or in both, or select a method, category, or action, or any combination of them from the drop-down lists, and enter this using the **Enter** key of your keyboard.

  The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go. To delete all entries, select the **Select all** checkbox and click this button.

  The list will then display only entries matching the filter.

- **Move Up, Move Down** — Select the entry you wish to move by selecting the **Select** checkbox next to it and click either of these buttons, depending on where you want to move the entry.

  The position an entry takes in the list is important since whenever more than one of the entries, such as rules, in the list match a request, the entry that is first in the list wins.

  This means that all following entries are ignored unless the **Continue** option is set.
FTP Command Filter List

The FTP Command Filter List options are invoked by clicking on the corresponding button under Common.

If you want to enable any of these options, make sure the checkbox on this button is also selected. The checkbox is selected by default. After modifying the setting of this checkbox, click Apply Changes to make the modification effective.

These are policy-dependent options — they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled Policy, which is located above the Media Type Filters button:

<table>
<thead>
<tr>
<th>Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
</tr>
<tr>
<td>Media Type Filters</td>
</tr>
</tbody>
</table>

The options are described in the upcoming section:

- FTP Command Filter List

FTP Command Filter List

The FTP Command Filter List tab looks like this:

There is the following section on this tab:

- FTP Command Filter List
FTP Command Filter List

Using this section, you can configure rules for assigning actions to particular FTP commands that occur in user requests and add these rules to a list. The rules may also include a categorization of the command and specify the URL it is applied to.

For example, you could set up a rule that categorizes a Server Access command when applied to a particular URL as chat and blocks the corresponding request.

Rules are not configured here for individual commands, but rather for command categories, such as the category of Server Access or Download commands.

The command categories used here include the following FTP commands:

<table>
<thead>
<tr>
<th>Command Category</th>
<th>FTP Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Access</td>
<td>USER, LIST, NLIST</td>
</tr>
<tr>
<td>Partial</td>
<td>REST, APPE</td>
</tr>
<tr>
<td>Download</td>
<td>RETR</td>
</tr>
<tr>
<td>Upload</td>
<td>APPE, STOR, STOU, MKD, ALLO</td>
</tr>
<tr>
<td>Rename</td>
<td>RNFR, RNTO</td>
</tr>
<tr>
<td>Delete</td>
<td>DELE, RMD</td>
</tr>
<tr>
<td>Site</td>
<td>SITE</td>
</tr>
</tbody>
</table>

To add a rule to the list, use the area labeled:

- **Add rule**

  Use the following items to configure the rule:

  - **Command category** — From this drop-down list, select the command category you want to configure a rule for.
    
    When selecting the Site command category, enter the command that should be executed on the FTP server in the input field next to the list. The rule will then need this command to match.
    
    Entering an * here means that the command category part of the rule will match for any command that is sent to the FTP server, using the SITE command.

  - **URL** — In this input field, enter the URL that is requested when the command is used. Input in this field is optional.

  - **Category** — From this drop-down list, select a URL filtering category you want to assign to the command. Setting this category is also optional.

  - **Action** — From this drop-down list, select the action you want to have executed if the rule matches.

  - **Continue** — If this checkbox is selected, McAfee Web Gateway will look for further matches after the rule matched for the first time. Otherwise, filtering activities will be stopped after the first match.

  - **Description** — Enter a description of the rule here. Input in this field is optional.

  - **Add to FTP Method Filter List** — After specifying the appropriate information in the fields above, click this button to add the rule to the list.
    
    The rule will be valid only under the policy you are currently configuring. To add a rule to the list that is valid for all policies, select the checkbox labeled **Add to all policies** before clicking on the button.
The FTP Command Filter List is displayed at the bottom of the section. To display only a particular number of list entries at a time, type this number in the input field labeled Number of entries per page and enter it using the Enter key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the URL or Description column or in both, select the appropriate method, category, and action from the drop-down lists, and enable or disable the Continue option.

Then click Apply Changes to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filtering term in the input field of the URL or Description column or in both, or select a command, URL filtering category, or action, or any combination of them from the drop-down lists, and enter this using the Enter key of your keyboard.

  The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the Select checkbox next to it and click this button. You can delete more than one entry in one go. To delete all entries, select the Select all checkbox and click this button.

  The list will then display only entries matching the filter.

- **Move Up, Move Down** — Select the entry you wish to move by selecting the Select checkbox next to it and click either of these buttons, depending on where you want to move the entry.

  The position an entry takes in the list is important since whenever more than one of the entries, such as rules, in the list match a request, the entry that is first in the list wins.

  This means that all following entries are ignored unless the Continue option is set.

---

Welcome page

The Welcome Page options are invoked by clicking on the corresponding button under Common.

If you want to enable any of these options, select the checkbox that is on this button. Then click Apply Changes to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled Policy, which is located above the Media Type Filters button:

<table>
<thead>
<tr>
<th>Policy:</th>
<th>Media Type Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>✓</td>
</tr>
</tbody>
</table>

The options are described in the upcoming section:

- Welcome page
Welcome page

The Welcome Page tab looks like this:

<table>
<thead>
<tr>
<th>Welcome page options</th>
<th>Defined options for this policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define when and how often the welcome page should be shown</td>
<td></td>
</tr>
<tr>
<td>- Show once a day at 7:00</td>
<td></td>
</tr>
<tr>
<td>- Show each 360 minutes</td>
<td></td>
</tr>
<tr>
<td>- Opt out</td>
<td></td>
</tr>
<tr>
<td>- User must acknowledge Welcome page before continuing</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manipulate user history</th>
<th>Allows to set options for one individual user</th>
</tr>
</thead>
<tbody>
<tr>
<td>User identifier:</td>
<td>(Format: login name or IP address)</td>
</tr>
<tr>
<td></td>
<td>Show again</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upload</th>
<th>Allows to upload the welcome page content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename:</td>
<td></td>
</tr>
<tr>
<td>Store as:</td>
<td>index.html</td>
</tr>
<tr>
<td></td>
<td>Add or overwrite content</td>
</tr>
<tr>
<td></td>
<td>Replace complete folder</td>
</tr>
<tr>
<td></td>
<td>Show updated page immediately</td>
</tr>
</tbody>
</table>

There are three sections on this tab:

- Welcome Page Options
- Manipulate User History
- Upload

Welcome Page Options

The Welcome Page Options section looks like this:

Using this section, you can configure options for the Welcome Page. You can configure the time and frequency of its appearance and also if it should appear at all.

A template of the Welcome page is stored under \conf\welcome\default after installation of the McAfee Web Gateway software. The file name is index.html, unless the Acknowledge option is configured, see below. You can also modify this page to make it suit your requirements.
After modifying the settings in this section, click **Apply Changes** to make the modification effective.

Use the following items to configure the Welcome Page options:

- **Show once a day at ...** — To let the Welcome Page appear only once a day, make sure the radio button provided here is checked and enter the time of appearance in the input field.
  
  Use the 24-hours format to enter a time, for example, 1 p.m. = 13:00.

- **Show each ... minutes** — To let the Welcome Page appear after a particular time interval has elapsed, select the radio button provided here and enter the time interval (in minutes) in the input field.

- **Opt out** — If this checkbox is selected, the Welcome Page will not appear in sessions of the user who configured this setting.

- **User must acknowledge Welcome page before continuing** — If this checkbox is selected, the user needs to click the **Yes ...** button on the Welcome page to continue.
  
  In this case, a different page is shown. Its name is `welcomeack.html` and it is also stored under `conf\welcomepage\default`, see above.

### Manipulate User History

The **Manipulate User History** section looks like this:

- **Manipulate user history**
  - Allows to set options for one individual user

<table>
<thead>
<tr>
<th>User identifier:</th>
<th>Show again</th>
<th>Show never again</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Format: user name or 192.168.67.33)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using this section, you can configure options for the Welcome Page with regard to an individual user. You can configure that the Welcome Page is displayed to this user or not. If it is displayed, the options of appearance configured in the Welcome Page Options section above apply.

After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following items to configure Welcome Page options for an individual user:

- **User identifier** — In this input field, enter information to identify the user. This can either be the IP address of the user’s system or the authenticated user name.
  
  The Welcome Page will then be displayed to this user or not, depending on which of the two buttons described below you click.

- **Show again** — Click this button to let the Welcome Page appear again for this user. This means that the page is displayed not only once, but also for the following requests of this user.

- **Show never again** — Click this button to hide the Welcome Page from this user.

### Upload

The **Upload** section looks like this:

- **Upload**
  - Allows to upload the welcome page content

<table>
<thead>
<tr>
<th>Filename:</th>
<th>Browse</th>
<th>Upload</th>
</tr>
</thead>
</table>

  Store as: **index.html** (Needed only if uploads)

- **Add or overwrite content**
- **Replace complete folder**
- **Show updated page immediately**
Using this section, you can configure and perform the upload of a file to display its content on the Welcome Page. Furthermore, you can let the Welcome Page appear immediately after the upload, regardless of what was configured in the other sections of this tab.

Use the following items to handle the upload of a Welcome Page:

- **Filename** — In this input field, enter the name of the file you want to upload. Type the file name or use the **Browse** button next to the input field to browse to the file. Then click **Upload** to perform the upload.

- **Store as** — In this input field, enter the name you want store the uploaded file under. If you are uploading an archive, you need not enter a name here since the file name will be used that is in the archive.

- **Add or overwrite content** — To add the content of the uploaded file to the Welcome Page or have its content overwritten by the uploaded content, make sure this radio button is checked. The radio button is checked by default.

- **Replace complete folder** — To delete all old files providing content for the Welcome Page prior to the upload, select this checkbox.

- **Show updated page immediately** — To let the Welcome Page appear immediately after the upload, regardless of the settings in the other sections of this tab, make sure this checkbox is selected. The checkbox is selected by default.

---

**White List**

The **White List** options are invoked by clicking on the corresponding button under **Common**. These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **Media Type Filters** button:

<table>
<thead>
<tr>
<th>Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
</tr>
<tr>
<td>Media Type Filters</td>
</tr>
</tbody>
</table>

The options are described in the upcoming sections:

- **White List**
- **Large file limits**
Common
White List

White List

The **White List** tab looks like this:

![White List Tab Image]

There is the following section on this tab:

- **White List**

**White List**

Using this section, you can configure the White List, which allows you to exclude various filters from being applied to particular objects.

This is done by specifying a string that is contained in an object, as well as the object type and the filters that should not be applied. There is a list of filters provided here, which you can disable and enable them according to your requirements.

Use the following items to configure the White List:

- **Add new entry** — Use the items in this area to specify the objects that should be exempted from filtering and the filters that should not be applied to them:
  - **String - International Domain Name** — Select one of these two string categories here and enter a shell expression or an international domain name string accordingly in the input field next to the categories field.
If you want to enter non-ASCII characters and the string should be used for the domain part of an URL, use the International Domain Name (IDN string) type.

In some countries like Germany, Sweden, or Japan, domain names with non-ASCII characters are allowed. There is a standard available (IDNA - International Domain Names in Applications) describing how a Web browser converts such a domain name entered by the user into a pure ASCII notation used by DNS and other devices.

McAfee Web Gateway has to use the pure ASCII notation as well, therefore all IDN strings must be converted before they can be used by McAfee Web Gateway. This is done automatically, if you select International Domain Name and enter a string with non-ASCII characters.

Note: You can not use shell expressions with IDN strings.

- None - Web ... — Select a category from this drop-down list in order to specify the kind of objects that should not be filtered when containing the string or international domain name specified above. Then make a further specification by selecting an appropriate restriction from the other drop-down list in this row. The restrictions you can select here vary according to what was selected from the first list.

So if you first select Web, this can be further specified by Any URL, URL Category, HTTP Request URL, and so on.

- Example 1 – Whitelisting Microsoft updates
  You want to whitelist Microsoft updates in order to make sure they are not blocked when downloaded to your network.
  Select String in the upper row and enter the generic file name for such updates in the field next to it, which might be download.windowsupdate.com/ *.cab.
  In the lower row, select Web and Any URL.

- Example 2 – Whitelisting based on the header content length
  You want to whitelist objects where the header has a content-length that exceeds a certain value. Select String in the upper row, as well as Header and Content length greater than in the lower. In the second input field of the upper row, enter the value that may be exceeded. The unit is always bytes here and must be omitted when entering the value, for example, for 7200 bytes enter 7200.

- Example 3 – Disabling the Progress Pages for PDF files
  You want to use the White List to ensure the progress made when a large PDF file is downloaded is not shown on a Progress Page.

  When the Progress Page is the preferred method for progress indication, an HTML Web page will be displayed with the progress of the download and a notification when the download is completed. The problem with PDF depends on the Adobe PDF Reader installed. Almost all installations deliver a browser plugin, which is executed when you hit a PDF download link on a Web page a and tries to download the PDF file to display it.

  McAfee Web Gateway then delivers the Progress Page instead of the PDF file, and the PDF reader receives a formatted HTML site instead of the requested PDF file. However, as the PDF reader is not able to display the HTML content, a blank page will be displayed.

  To solve this problem, you need to prevent the Progress Page from serving as progress indication method for PDF files and use the Data Trickling method instead. This means you need to whitelist the Progress Page.
Select **String** in the upper row, as well as **Media Type** and **Ensured Type** in the lower.

In the second input field of the upper row, enter *application/pdf*.

Furthermore, select the **Progress Page** checkbox in the list provided under **Disable**, see also the next item.

- **Disable** — From the list of filters and anti-virus engines provided here disable those that should not be applied to the specified object by selecting the checkboxes next to them.

  You can disable any combination of the list items, for example, the Media Type Filter, Spam Filter, and Web Reputation Filter.

- **Description** — Enter a text here describing the type of objects that should not be filtered. Input in this field is optional.

- **Add to White List** — After specifying the above settings, click this button to add them as entry to the White List.

  If you want to make these settings effective under all policies, select the **Add to all policies** checkbox before clicking **Add to White List**.

The White List is displayed at the bottom of the section. To display only a particular number of entries at a time, type this number in the **Number of entries per page** input field and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the corresponding input fields and select or deselect the checkboxes of the filters and anti-virus engines you want to exclude from being applied.

The first of the three input fields provided here contains the shell expression string that is entered when specifying the kind of objects in question. The third input field contains the plain-text description, and the second field, which contains the type specifications, cannot be altered.

Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filter term in this input field and enter it using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.

- **Move Up, Move Down** — Select the entry you wish to move by selecting the **Select** checkbox next to it and click either of these buttons, depending on where you want to move the entry.

  The position an entry takes in the list is important since whenever there is more than one entry in the list containing information on a particular object, the entry that is first in the list wins.

  This means the White List settings of that entry are applied while all following entries are ignored.
**Filter Settings List**

The list below is a list that shows you where the settings of the various filters that can be disabled for entries on the White List are configured within this user interface.

The filters are listed in alphabetical order:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Settings are where configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveX Controls</td>
<td>Anti Malware &gt; Proactive Scanning &gt; Configuration: ActiveX Controls row in Behavioral Heuristics section</td>
</tr>
<tr>
<td>Advertising Filter</td>
<td>Common &gt; Advertising Filters</td>
</tr>
<tr>
<td>Archive Handler</td>
<td>Common &gt; Archive Handler</td>
</tr>
<tr>
<td>Attachment Filter</td>
<td>Anti Spam &gt; Message Filters &gt; Settings: Section/Attachment Filter section and ... &gt; Attachment Filter List</td>
</tr>
<tr>
<td>Authenticode</td>
<td>Anti Malware &gt; Authenticode</td>
</tr>
<tr>
<td>AV Engines (ETrust, McAfee, Secure Anti-Malware, Sophos, All AV engines)</td>
<td>Anti Malware &gt; Virus Scanning</td>
</tr>
<tr>
<td>Data Trickling</td>
<td>Proxies &gt; Progress Indication Methods: Data Trickling section</td>
</tr>
<tr>
<td>Document Inspector</td>
<td>Common &gt; Document Inspector</td>
</tr>
<tr>
<td>Embedded Objects</td>
<td>Anti Malware &gt; Embedded Objects</td>
</tr>
<tr>
<td>Embedded Scripts</td>
<td>Anti Malware &gt; Embedded Scripts</td>
</tr>
<tr>
<td>Filter by Expressions</td>
<td>URL Filter &gt; Filter by Expressions</td>
</tr>
<tr>
<td>Generic Body Filter</td>
<td>Common &gt; Generic Body Filter</td>
</tr>
<tr>
<td>Generic Header Filter</td>
<td>Generic Header Filter</td>
</tr>
<tr>
<td>HTTP Cache</td>
<td>Caching &gt; HTTP Caching</td>
</tr>
<tr>
<td>Media Type Filter</td>
<td>Common &gt; Media Type Filters</td>
</tr>
<tr>
<td>Privacy Filter</td>
<td>Common &gt; Privacy Filters</td>
</tr>
<tr>
<td>Proactive Scanning</td>
<td>Proactive Scanning - Anti Malware &gt; Proactive Scanning</td>
</tr>
<tr>
<td>Progress Pages</td>
<td>Proxies &gt; Progress Indication Methods: Progress Pages section</td>
</tr>
<tr>
<td>Recipient Filter</td>
<td>Anti Spam &gt; Message Filters: Recipient Filter section</td>
</tr>
<tr>
<td>Sender Filter</td>
<td>Anti Spam &gt; Message Filters: Sender Filter section</td>
</tr>
<tr>
<td>Size Filter</td>
<td>Anti Spam &gt; Message Filters: Size Filter section</td>
</tr>
<tr>
<td>Spam Filter</td>
<td>Anti Spam &gt; Spam Filter Methods</td>
</tr>
<tr>
<td>Subject Filter</td>
<td>Anti Spam &gt; Message Filters: Subject Filter section</td>
</tr>
<tr>
<td>Text Categorization</td>
<td>Common &gt; Text Categorization</td>
</tr>
<tr>
<td>URL Category Actions</td>
<td>URL Filter &gt; Category Actions</td>
</tr>
<tr>
<td>Web Reputation Filter</td>
<td>URL Filter &gt; Web Reputation</td>
</tr>
</tbody>
</table>
Large file limits

The **Large File Limits** tab looks like this:

There is the following section on this tab:

- **Large file limits**

**Large file limits**

Using this section, you can limit the amount of data that is read into the main memory of your system when a file is transferred to it. Furthermore, you can determine what should happen to large files that exceed the limit.

Some of the McAfee Web Gateway filters work on data stored in the main memory. This means that in order to be processed by one of these filters, a file must be read into the main memory first. If the file is large enough to exceed the limit that has been set here, it will be blocked by default since no unfiltered object should be allowed to pass through in general.

This default procedure can be bypassed, however, by configuring a setting that allows such large files to pass through without any filtering.

**Note:** The settings described here do not affect filters such as, for example, the ones that are provided by the anti-virus engines because these work on data stored on disk, not in main memory.

After modifying the settings of this section, click **Apply Changes** to make the modification effective.

Use the following items to configure large file settings:

- **Maximum size in memory . . . MB** — In this input field, enter the maximum size for a file (in megabytes) that may be read into the main memory of your system.

- **Allow files that are larger than specified above** — Select this checkbox to allow large files that exceed the limit configured above.

These files will then pass through without filtering because, due to the size limit, they are not read into the main memory.
User defined categories

The User Defined Categories options are invoked by clicking on the corresponding button under Common. They are described in the upcoming section:

- User defined categories

User defined categories

The User Defined Categories tab looks like this:

<table>
<thead>
<tr>
<th>User-Defined Categories</th>
<th>Names and abbreviated categories (to be written to the log file)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of user defined categories</td>
<td>5 (up to 500)</td>
</tr>
<tr>
<td>Category 1: User-Defined 1</td>
<td>UD-1</td>
</tr>
<tr>
<td>Category 2: User-Defined 2</td>
<td>UD-2</td>
</tr>
<tr>
<td>Category 3: User-Defined 3</td>
<td>UD-3</td>
</tr>
<tr>
<td>Category 4: User-Defined 4</td>
<td>UD-4</td>
</tr>
<tr>
<td>Category 5: User-Defined 5</td>
<td>UD-5</td>
</tr>
</tbody>
</table>

There is the following section on this tab:

- User Defined Categories

User Defined Categories

Using this section, you can configure your own categories for URL classification with names and abbreviated name formats. You can configure up to 500 categories this way.

The abbreviated format is needed for two purposes: log files and the X-Attribute header. The X-Attribute header is a type of REQMOD/RESPMOD header, and is a compatibility setting used to simplify the cooperation between the ICAP server and client.

After changing an abbreviated name (all the possible values of the X-Attribute header will be sent in the OPTIONS response), ICAP clients may run into problems until the next OPTIONS request if they rely on previous OPTIONS responses.

The categories that you configure here will be shown on the Category Actions tab under URL Filter > Category Actions, where you can configure actions for these categories.

After specifying the appropriate settings, click Apply Changes to make them effective.
Use the following items to configure categories:

- **Number of user defined categories** — In the input field provided here, enter the number of categories you want to configure. The maximum number is 500, the default is 5.

  Then click **Apply Changes** for the first time. You need to click this button a second time after specifying the settings for the individual categories.

  The list of category input fields will then be enlarged or reduced according to the number you entered.

- **Category 1, Category 2, ...** — In the input fields provided here enter the category names you want to use and the abbreviated formats of these names.
**Media Type Catalog**

The **Media Type Catalog** options are invoked by clicking on the corresponding button under **Common**. They are described in the upcoming section:

- **Media Type Catalog**

**Media Type Catalog**

The **Media Type Catalog** tab looks like this:

![Media Type Catalog Tab](image)

There is the following section on this tab:

- **Media Type Catalog**
Media Type Catalog

Using this section, you can add media types to the Media Type Catalog or modify media types that are already in the catalog.

A media type is a general category of data content, such as an application, audio content, a text message, an image, or a video stream. The media type tells the application that receives the data what kind of application is needed to process the content; for example, audio means the audio content should be played for the user.

Each of these media types also has subtypes, for example, the text media type has plain, html, xml, and others.

You can also specify the magic byte sequences that files belonging to a particular media type should have.

The following area is provided for adding a media type to the catalog or modifying it:

- **Add or modify Media Type** — Use the following items to do this:
  - **File Extensions** — In the input field provided here, enter the extension that files of the media type in question will have. If you specify several extensions, separate them by commas, for example, enter jpg, jpeg for the image/jpeg media type.
  - **Options** — Configure the following options by selecting the corresponding checkboxes:
    - **Magic bytes are necessary** — Select this checkbox to ensure that a file will only be detected by McAfee Web Gateway as belonging to a particular media type if it contains the corresponding magic byte sequence.
      
      This sequence is specified further below under **Magic Bytes**. If more than one sequence is specified there, one match is sufficient for McAfee Web Gateway to detect the media type.
      
      For example, to detect the application/zip media type, it could be required that a file contains 504B0304 as magic byte sequence.
    - **Magic bytes are ambiguous** — Select this checkbox to ensure that an additional routine is executed by McAfee Web Gateway to detect a media type after finding a particular magic byte sequence in a file.
      
      This is required in case the magic byte sequence is ambiguous, which means it is used to identify more than one particular media type. Sometimes an examination of the whole file is then needed to detect the exact type.
      
      Again, the magic byte sequence in question is entered under **Magic Bytes**. If more than one sequence is specified there, one match will be sufficient for McAfee Web Gateway to start the additional routine for detecting the exact media type.
      
      An example of media types with ambiguous magic bytes are those of the Microsoft Office family, application/msword, application/msexcel, application/mspowerpoint, and so on. A file belonging to one of these media types always has D0CF11E0A1B11AE1 at its beginning and an additional magic byte sequence at its end.
      
      If this option is enabled, it tells McAfee Web Gateway that the magic byte sequence at the beginning of such a file is ambiguous and that some extra processing is needed.
      
      The sequence also tells McAfee Web Gateway that the file is a Microsoft Office document. So, if a setting is configured within McAfee Web Gateway that blocks all objects of that kind, this will be executed accordingly.
      
      If this is not so, and further processing is appropriate, McAfee Web Gateway activates the filter that is suitable for the object, which is the Document Inspector in this case.
      
      The Document Inspector may need to know the subtype of the file, msword, msexcel, mspowerpoint, and so on, and performs the operations that are required to detect it. The whole file may get examined then for this purpose.
After detecting the subtype, the filter goes on to process the file according to the settings that have been configured.

- **Magic Bytes** — In the input fields of the columns provided here, enter up to five magic byte sequences and their offsets to identify a media type:
  - **Offset** — In this column, enter the offset values for the magic byte sequences.
    - If you are not sure about the offset of a magic byte sequence because it might begin anywhere in the file, enter -1 as offset value.
  - **Magic Bytes** — In this column enter the values for the magic byte sequences themselves.
  - **Add/Modify** — After specifying the information for a media type, click this button to add it to the catalog.

The list of media types included in the Media Type Catalog is displayed at the bottom of this section. To display only a particular number of list entries at a time, type this number in the **Number of entries per page** input field and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To view the details of an entry or modify them, click the **view details or edit** in the same line. This will display the information that was configured for it in the input fields and checkboxes of the upper part of the section, where you can modify it according to your requirements.

After modifying this information, click **Add/Modify** to make the modification effective. You can modify more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filtering term in the input field of the **Media Type** column at the top of the list and enter it using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go.

  To delete all entries, select the **Select all** checkbox and click this button.
URL Filter

Contents
Filtering web traffic
Quick snapshot
URL filtering methods
Category actions
Quotas and coaching
Filter by expressions
Web reputation
Extended List Manager
Category scheme
Progressive lockout
GTI settings

Filtering web traffic
The features that are described in this chapter are accessible over the URL Filter tab of the user interface:

These features allow you to configure the filtering of Web sites and the blocking of certain categories of them, such as travel, entertainment, or gambling.

Quick snapshot
The Quick Snapshot for the URL filtering functions is invoked by clicking on the corresponding button under URL Filter. The options of this feature are described in the upcoming sections:

- Categories
- Web reputation

Before this is done, however, the following subsection provides some general information about the quick snapshot features.

Handling the quick snapshot
The quick snapshot features allow you to view summary information on the URL filtering performed by McAfee Web Gateway (formerly Webwasher®) at a glance. Part of the information is displayed with regard to a given time interval.
Percentages are calculated for the categories that the filtered URLs belonged to with regard to frequency and volume. The percentages are shown by means of a pie chart on the left side of a section.
On the right side of a section, values are shown as they developed in time, using either a stacked or a line mode.
The pie chart and the representation in stacked or line mode are handled in the same way as on the McAfee Web Gateway dashboard.
You can:

• Select and deselect categories for display by selecting and deselecting the corresponding checkboxes:

  ![Checkbox images](image)

  text/html
  text/plain
  video/x-ms-wmv

• Select a time interval for display, using the **Show last** drop-down list:

  ![Dropdown image](image)

• Select stacked or line mode for display by checking the corresponding radio button:

  ![Radio buttons image](image)

  **Stacked**  **Line**

For a more detailed description of these activities, see the subsection labeled *Handling the dashboard* in the *Dashboard* section under *Home*.

There is, however, a property of the quick snapshot features that is not present on the dashboard tabs:

**Resetting top value lists**

For the *Categories by Hits*, *Categories by Volume* and *Top Uncategorized Sites* parameters on the *Categories* tab, as well as for the *Top Malicious Reputation Sites* on the *Web Reputation* tab, top value lists are displayed.

These use the length of bars to indicate the number of hits or the amount of bytes for various categories.

You can choose to view the top 10, 25, etc., using a drop-down list:

  ![Dropdown image](image)

  **Top 10**
  **Top 25**
  **Top 50**
  **Top 100**
  **Top 200**
  **Top 500**

The top value lists can be reset with a reset button. After clicking on this button, all values in a list are set to zero, so the measurement of values can start all over again.

A timestamp is displayed, indicating date and time of the last reset.
Categories

The **Categories** tab is shown in two parts here because of its size. The upper part of the tab looks like this:

- **Categories by Hits**
  - Average (last 1 Hour)
  - Show last 1 Hour
  - Resolution: 1 minute
  - Stacked

- **Categories by Volume**
  - Average (last 1 Hour)
  - Show last 1 Hour
  - Resolution: 1 minute

- **Triggered Category Actions**
  - Average (last 1 Hour)
  - Show last 1 Hour

- **Category Groups by Hits**
  - Average (last 1 Hour)
  - Show last 1 Hour
The lower part looks like this:

```plaintext
{table}
<table>
<thead>
<tr>
<th>Category</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software / Hardware</td>
<td>95</td>
</tr>
<tr>
<td>Business</td>
<td>95</td>
</tr>
</tbody>
</table>

{table}
<table>
<thead>
<tr>
<th>Category</th>
<th>Bytes transferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software / Hardware</td>
<td>97.2kB</td>
</tr>
<tr>
<td>Business</td>
<td>97.2kB</td>
</tr>
</tbody>
</table>

There are seven sections on this tab:

- **Categories by Hits (over time)**
- **Categories by Volume (over time)**
- **Triggered Category Actions**
- **Category Groups by Hits**
- **Categories by Hits (top categories)**
- **Categories by Volumes (top categories)**
- **Top Uncategorized Sites**

**Categories by Hits (over time)**
This section displays the URL categories that were most often processed by the Webwasher URL Filter within a given time interval and how often each of them was processed.

**Categories by Volume (over time)**
This section displays the URL categories that were processed by the Webwasher URL Filter and consumed the greatest bandwidth volume.

**Triggered Category Actions**
This section displays the actions that were configured for particular actions and then triggered by the Webwasher URL Filter within a given time interval.

It is also displayed how often each of them was triggered.

**Category Groups by Hits**
This section displays the URL category groups that were most often processed by the Webwasher URL Filter within a given time interval and how often each of them was processed.

**Categories by Hits (top categories)**
This section displays a list of the URL categories that were most often processed by the McAfee Web Gateway URL Filter, showing also the number of hits for each of them.

Hit numbers are accumulated until the section is reset.
The following information is displayed for each category:

- **Category** — Name of the category
- **Hits** — Number of times that this category was processed by the McAfee Web Gateway URL Filter

**Categories by Volumes (top categories)**

This section displays a list of the URL categories that were processed by the McAfee Web Gateway URL Filter and consumed the greatest bandwidth volume.

Volumes are accumulated until the section is reset.

The following information is displayed for each category:

- **Category** — Name of the category
- **Bytes transferred** — Number of bytes transferred for URLs of that category

**Top Uncategorized Sites**

This section displays a list of sites that are identified by the domain name parts of their URLs. The URLs containing these domain names were processed by the Webwasher URL Filter, but not yet categorized within the URL Filter Database.

Whenever a URL is processed, a hit is counted for the corresponding site. Sites are ranked in the list according to their hit numbers. Hit numbers are accumulated until the section is reset.

The following information is displayed for each site:

- **URL (domain)** — Domain name part of a URL identifying a particular site and occurring in one or more URLs that were processed by the Webwasher URL Filter
- **Hits** — Number of times that an uncategorized URL with that domain name was processed
Web reputation

The Web Reputation tab looks like this:

Web Reputation by Hits

There are two sections on this tab:

- Web Reputation by Hits
- Top Malicious Reputation Sites

Web Reputation by Hits

This section displays the number of URLs for various degrees of Web reputation. URLs are processed by the McAfee Web Gateway URL Filter and given reputation scores, indicating to what degree URLs can be trusted.

The scores are provided by the TrustedSource Web Database, where a huge amount of data has been collected on millions of URLs.

Reputation scores range from -127 to +127.

Note: A high reputation score for a URL indicates that it is considered as probably malicious.

Invoking a malicious URL means that you are putting your system or its content at risk by going to the corresponding site. This is usually due to something malicious, which may be a virus, spyware, phishing, etc., but could also be due to something illegal about where you are going.

Furthermore, any score that is positive is an indication that there are still some doubts about the site in question, whereas a negative score means it is trustworthy.

Hit numbers are shown for the following degrees:

- Malicious — A URL with a reputation score of 50 or higher is classified as malicious. This means that the Web page in question contains malicious content or is not from a legitimate Web server.

- Suspicious — A URL with a reputation score of 30 to 49 is classified as suspicious. The Web page in question shows many characteristics associated with a malicious Web server and any content from it requires special scrutiny.
URL Filter
URL filtering methods

- **Unverified** — A URL with a reputation score of 15 to 29 is classified as unverified. The Web page may belong to a legitimate Web server, but displays a few properties suggesting further inspection is necessary.

- **Neutral** — A URL with a reputation score of 0 to 14 is classified as neutral. The Web page most likely belongs to a legitimate Web server, but all content requires further inspection.

- **Trusted** — A URL with a reputation score below zero is classified as trusted. The Web page belongs to a legitimate, secure Web server with no malicious content or risk of such content.

**Top Malicious Reputation Sites**
This section displays a list of sites that are identified by the domain name parts of their URLs. The URLs containing these domain names were processed by the McAfee Web Gateway URL Filter and classified as *malicious*, which means that the reputation score given to them was 50 or higher.

Whenever a URL is classified as malicious, a hit is counted for the corresponding site. Sites are ranked in the list according to their hit numbers. Hit numbers are accumulated until the section is reset.

The following information is displayed for each site:

- **URL (domain)** — Domain name part of a URL identifying a particular site and occurring in one or more URLs that were processed by the McAfee Web Gateway URL Filter

- **Hits** — Number of times that a URL with that domain name was classified as malicious

**URL filtering methods**

The **URL Filtering Methods** options are invoked by clicking on the corresponding button under **URL Filter**. If you want to enable any of these options, make sure the checkbox on this button is also selected. The checkbox is selected by default.

After modifying the setting of this checkbox, click **Apply Changes** to make the modification effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **URL Filtering Methods** button:

```
<table>
<thead>
<tr>
<th>Policy:</th>
<th>URL Filtering Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>✓</td>
</tr>
<tr>
<td>URL Filtering Methods</td>
<td>✓</td>
</tr>
</tbody>
</table>
```

The options are described in the upcoming section:

- **URL filtering methods**
URL filtering methods

The **URL Filtering Methods** tab looks like this:

URL Filtering Methods

- URL Filtering Methods - Selects databases to use for URL classification
  - URL Filter Database - Blocks URLs according to their categories
    - Skip searching the CGI parameters when categorizing URLs.
    - Skip searching for and categorizing embedded URLs.
    - Skip additional categorization of a search engine request, such as a query to Google, based on the keywords present in the search.
  - Extended List - Blocks URLs based on your own list entries

- Real-Time Classifier - Classifies pornography and nudity based on the URL or meta information
  - URL Based Classification - Classifies pages based on their URL
    - Confidence level required for blocking: Low ○ ○ ○ ○ High
  - Meta Information Based Classification - Classifies pages based on their meta information
    - Confidence level required for blocking: Low ○ ○ ○ ○ High
  - Real-Time Classifier Options - Defines the threshold to be compared with the sum of both classification methods
    - Overall confidence level required for blocking: Low ○ ○ ○ ○ High

- SafeSearch Enforcer - Enforces the usage SafeSearch/FamilyFilter options of search engines
  - Enforce moderate filtering (only multimedia content)
  - Enforce strict filtering (all content types)

- Default Action - Allow or block remaining unfound URLs
  - Default action for URLs not covered by any method: Allow

There are four sections on this tab:

- **URL Filtering Methods**
- **Real-Time Classifier**
- **SafeSearch Enforcer**
- **Default Action**

**URL Filtering Methods**

The **URL Filtering Methods** section looks like this:

URL Filtering Methods

- URL Filtering Methods - Selects databases to use for URL classification
  - URL Filter Database - Blocks URLs according to their categories
    - Skip searching the CGI parameters when categorizing URLs.
    - Skip searching for and categorizing embedded URLs.
    - Skip additional categorization of a search engine request, such as a query to Google, based on the keywords present in the search.
  - Extended List - Blocks URLs based on your own list entries
Using this section, you can configure the use of the URL Filter Database that is provided by McAfee. You can also configure the use of the Extended List, which allows you to include additional URLs in the filtering process.

In the URL Filter Database, millions of URLs have been entered and categorized in different categories. When a user tries to access a Web site, the corresponding URL is filtered against what is in the database. If the filter matches, actions such as Block, Delay, Allow, etc. can be executed.

So if a user tries to access a Web site where the URL has been categorized, such as Online Shopping, and Block was configured as action for this category, the URL is blocked and the user will not get access to that site. A notification is then displayed to inform the user about the blocking.

You can update the URL Filter Database using the update manager functions, which are provided by Webwasher on the **URL Filter** tab under **Configuration > Update Manager**. To go there, you may also just click the link at the bottom of this page.

The Extended List enables you to list additional URLs and the corresponding categorizations, using the categories that are also applied within the URL Filter Database. URLs are then filtered not only against what is in the database, but also against this list.

**Note:** In conflicting cases, the Extended List receives higher priority than the URL Filter Database.

To add URLs to the Extended List, go to the **Extended List Manager** tab under **URL Filter > Extended List Manager**.

After modifying the settings in this section, click **Apply Changes** to make the modification effective.

Use the following checkboxes to configure the use of the URL Filter Database and the Extended List:

- **URL Filter Database** — If you want Webwasher to use the entries and categorizations stored in the URL Filter Database for filtering, make sure this checkbox is selected. The checkbox is selected by default.
  
  You can improve performance if you allow Webwasher to skip the filtering for some of the features and parameters a URL may have. To do this select the following checkboxes:

  - **Skip searching the CGI parameters when categorizing URLs.** — Select this checkbox to let Webwasher perform a filtering where the CGI parameters of a URL are ignored.
  
  - **Skip searching for and categorizing embedded URLs.** — Select this checkbox to let Webwasher perform a filtering where embedded URLs within a URL that is filtered are ignored.
  
  - **Skip additional categorization of a search engine request, such as a query to Google, based on the keywords present in the search.** — Select this checkbox to let McAfee Web Gateway perform a filtering where keywords in search engine requests are ignored.

- **Extended List** — If you want to use the Extended List, make sure this checkbox is selected. The checkbox is selected by default.

### Real-Time Classifier

The **Real-Time Classifier** section looks like this:

<table>
<thead>
<tr>
<th>Real-Time Classifier Options</th>
<th>Classifies pornography and nudity based on the URL or meta information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL Based Classification</strong></td>
<td>Classifies pages based on their URL. Confidence level required for blocking: Low</td>
</tr>
<tr>
<td><strong>Meta Information Based Classification</strong></td>
<td>Classifies pages based on their meta information. Confidence level required for blocking: Low</td>
</tr>
<tr>
<td><strong>Real-Time Classifier Options</strong></td>
<td>Defines the threshold to be compared with the sum of the scores of all scanners.</td>
</tr>
</tbody>
</table>

Using this section, you can configure the Real-Time Classifier to filter content based on URL or meta information.
You can also set a confidence level to evaluate these filtering activities.

The Real-Time Classifier classifies pornographic content based on the URL and on meta information. In the first step, it searches for keywords in a domain name or URL (URL-based classification).

If it is not blocked due to the entries in the URL Filter Database and the URL cannot be classified, the filter will receive the content of the Web site in order to make a keyword classification using metatag keywords.

After specifying the appropriate settings, click **Apply Changes** to make them effective.

Use the following checkboxes and radio buttons to configure the Real-Time Classifier:

- **URL Based Classification** — If you want to use this kind of classification, make sure this checkbox is selected. The checkbox is selected by default.

  Then set the confidence level by selecting the corresponding radio button.

  There are five different levels here, ranging from Low to High.

  A high confidence level would mean that keywords would not rely on single hit classification, due to the fact that these words could have another significance.

  For example, *teen* on its own is fine, but *teen + porn* is probably not. A low confidence level means keywords that require only one hit for them to be classified.

- **Meta Information Based Classification** — If you want to use this kind of classification, make sure this checkbox is selected. The checkbox is selected by default.

  Then set the confidence level by selecting the corresponding radio button.

  There are five different levels here, ranging from Low to High.

- **Real-Time Classifier Options** — If you want to use these options, make sure this checkbox is selected. The checkbox is selected by default.

  Then set the overall confidence level by selecting the corresponding radio button. There five different levels here, ranging from Low to High.

  The overall confidence level is applied to the combined result of the URL and the meta information-based classification methods configured above.

  If only one classification method is enabled, this option will not work even if you enable it.

  You may want to set the overall confidence level higher than levels of the two classification methods for more consistent blocking.

  If the individual methods themselves are uncertain as to whether a page may be pornographic in nature, the page can still be blocked due to the overall confidence level.

**SafeSearch Enforcer**

The **SafeSearch Enforcer** section looks like this:

- **SafeSearch Enforcer** — Enforces the usage SafeSearch/FamilyFilter options of search

  - Enforce moderate filtering (only multimedia content)
  - Enforce strict filtering (all content types)

Using this section, you can enable the use of the SafeSearch Enforcer to enable the filter of the search engine that excludes adult sites from search results.

Many search engines have a feature named SafeSearch, FamilyFilter, or similarly for excluding adult sites from search results.

You can configure McAfee Web Gateway to make use of this filter, but should be aware that Webwasher has no influence on the filter output.
You can configure a moderate and a strict filtering option. However, some search engines do not distinguish between moderate and strict filtering. Those engines will perform a standard filtering procedure, regardless of whether you have configured the moderate or the strict filtering option.

If you want to enforce the use of the SafeSearch feature, select the checkbox next to the section heading.

After specifying this setting or any other setting in this section, click **Apply Changes** to make these settings effective.

Use the following checkboxes to configure the severity level of the SafeSearch Enforcer:

- **Enforce moderate filtering (only multimedia content)** — Enable this option to filter only multimedia content, such as images, videos, etc.
- **Enforce strict filtering (all content types)** — Make sure this option is enabled if all results, including Web links, should be filtered. The option is enabled by default.

### Default Action

The **Default Action** section looks like this:

```
  Default Action  - Allow or block remaining unfound URLs
  Default action for URLs not covered by any method:  Allow
```

Using this section, you can configure a default action that is applied to URLs not covered by any other method configured on this tab.

After specifying the appropriate action, click **Apply Changes** to make this setting effective.

Use the following drop-down list to configure a default action for URL filtering:

- **Default action for URLs not covered by any method** — From this drop-down list, select the default action.

### Category actions

The **Category Actions** options are invoked by clicking on the corresponding button under **URL Filter**.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **URL Filtering Methods** button:

```
Policy:
  default
```

The options are described in the upcoming section:

- **Category actions**

This is followed by a section providing a list of suggestions for configuring categories with default actions to meet the requirements of a school, a business environment, an increased security policy and for other purposes:

- **Category defaults**

The suggestions recommend the use of an exempting action for some categories.

Since an action like this is not included among the built-in actions of McAfee Web Gateway, you need to configure it for yourself if you want to follow the suggestions in this respect.

A further section tells you how to configure this action:

- **Configuring an exempting action**
Category actions

The **Category Actions** tab looks like this:

There is the following section on this tab:

- **Category Actions**
**Category Actions**

Using this section, you can configure an action, such as Block, Allow, Allow on Weekends, and so on, that McAfee Web Gateway should execute whenever a URL of a given category, such as Pornography, Nudity, Drugs, and so on, is requested by a user.

You can configure actions for individual categories, as well as for groups of categories. Furthermore, you can configure a common action for all new categories, or even one for all categories.

A list of suggestions for configuring categories with default actions to meet the requirements of a school, a business environment, an increased security policy and for other purposes is provided under *Category defaults*.

In order to determine whether a URL falls into a particular category, McAfee Web Gateway relies on the entries in the TrustedSource Web Database, where millions of URLs are entered and categorized. The current version of the TrustedSource Web Database list of categories is displayed at the top of the section. The list is here referred to as "Category Scheme", and also as "SmartFilter Category Scheme", as the list is also used by the McAfee SmartFilter product, which is also used for URL filtering.

**Note:** If you have removed an older version of the McAfee Web Gateway software, which was up to the current version known under the name of Webwasher, from your system before installing version 6.5 of Webwasher, the current version of the TrustedSource Web Database list of categories is implemented as part of the new installation. The same is true if 6.5 is the first Webwasher version to be installed on your system.

After installing version 6.5, however, over an older Webwasher version, without removing this older version, the old Webwasher category scheme is retained. You may then upgrade to the TrustedSource Web Database list of categories or continue to use the old category scheme. It is, however, recommended to perform an upgrade.

If you continue to use the old category scheme, you need to perform a database update in order to make the URL filtering functions start working.

When the old category scheme is implemented, an alert is displayed at the top of this section to make you aware of the upgrade option. You can use the link that is displayed with the alert to go to the Category Scheme tab, where you can perform the upgrade.

To ensure URLs are filtered by McAfee Web Gateway according to the most recent information stored in that database updates are performed in regular intervals.

You can configure these updates on the **URL Filter** tab under **Configuration > Update Manager**. An alert is displayed if an update has not been performed for some reason or other.

You can then perform a manual update on the tab mentioned above. A link is displayed with the alert that gets you to this tab.

In addition to the categories that are listed on this tab and can be configured for URL filtering, you can use your own categories. Go to the **User-Defined Categories** tab under **Common > User Defined Categories** to set up these categories of your own.

Furthermore, you can add actions that you configured on your own to the list of actions provided for each category on this tab. This is done on the **Action Editor** tab under **Configuration > Action Editor**.

**Note:** With some actions, reference is made to a time scheme, such as Block during work hours. The times underlying a scheme are not configured on the tabs of this user interface, but by editing the corresponding entries in the global.ini (under Windows) or global.conf (under Linux and Solaris) configuration file.

These files include a section named [DynaBlock.TimeSchemes], where times are set up in 24-hours format corresponding to Always, Never, Non-Work Hours, and Weekend.

The default times are as follows:
- "Always" 00:00-24.00
- "Never" 00:00-08:00, 12:00-13:00, 17:00-24:00
- "Non-Work Hours" 00:00-24:00, 00:00-24:00 (the last two entries are for non-work hours on Saturdays and Sundays)
- "Weekend" A 00:00-24:00, S 00:00-24:00 (for Saturday and Sundays).

After modifying the default settings configured in the section on this tab, click **Apply Changes** to make the modification effective.

Use the following drop-down lists to configure actions for URL categories:

- **Default Action for new categories** — Select an action here that should be executed by default for new categories—for categories that were added to the category scheme after an update of the URL Filter Database, unless other actions have been configured for them.

- **Set ALL categories to** — Select an action here if you want to have the same action executed for all categories.
• **Pornography/Nudity** — From the drop-down lists provided here, select actions for the individual categories that are included in this group, such as Pornography, Nudity, Sexual Materials, etc.

Using the drop-down list in the same line as the group heading, you can also select an action that should be executed for all categories in this group.

• **Risk/Fraud/Crime, Drugs, etc.** — With all the other categories and category groups listed here, proceed in the same way as described under Pornography/Nudity.

### Category defaults

The table below contains a list of suggestions for configuring the McAfee Web Gateway category actions with default settings, but according to different purposes.

So, the defaults for a configuration that meets the requirements of a school will differ from one that is meant to be used in a typical business environment or one that should fulfill increased security standards.

The following combinations of default settings are provided for different purposes:

- Typical Minimum Configuration
- Typical School Configuration
- Typical Business Configuration
- Increased Productivity
- Increased Security
- Increased Bandwidth Protection

The categories are listed in alphabetical order. Furthermore, note that:

- An * means that Block should be selected as an action for the category.
- An X means that the category should be Exempt.
- An * in the School column means that the category should be Block or Exempt for a high school configuration.

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Typical minimum configuration</th>
<th>Typical school configuration</th>
<th>Typical business configuration</th>
<th>Increased productivity</th>
<th>Increased security</th>
<th>Increased bandwidth protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcohol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymizers</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Anonymizing Utilities</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Art/Culture/Heritage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auctions/Classifieds</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blogs/Wiki</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chat</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal Activities</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dating/Personals {NEW}</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dating/Social Networking</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Postcards</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drugs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Education/Reference</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extreme</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fashion/Beauty</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance/Banking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## URL Filter
### Category actions

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Typical minimum configuration</th>
<th>Typical school configuration</th>
<th>Typical business configuration</th>
<th>Increased productivity</th>
<th>Increased security</th>
<th>Increased bandwidth protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Kids</td>
<td>E</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forum/Bulletin Boards</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Gambling Related</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Game/Cartoon Violence</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Games</td>
<td>X*</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General News</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government/Military</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gruesome Content</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hacking/Computer Crime</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hate/Discrimination</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Health</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Historical Revisionism</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>E*</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Humor/Comics</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illegal Software</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Incidental Nudity</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Messaging</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interactive Web Applications</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Radio/TV</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Services</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job Search</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Sites</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing/Merchandising</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Downloads</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Sharing</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messaging</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderated</td>
<td>E*</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motor Vehicles (NEW)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Profit/Advocacy/NGO</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nudity</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Online Shopping</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P2P/File Sharing</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Parked Domain</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Network Storage</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Pages</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pharmacy</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Politics/Opinion</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category Name</td>
<td>Typical minimum configuration</td>
<td>Typical school configuration</td>
<td>Typical business configuration</td>
<td>Increased productivity</td>
<td>Increased security</td>
<td>Increased bandwidth protection</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>--------------------------------</td>
<td>-------------------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Pornography</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Portal Sites</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profanity</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Professional Networking (NEW)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provocative Attire</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Public Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Estate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Recreation/Hobbies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Religion/Ideology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remote Access</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Resource Sharing</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restaurants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>School Cheating Information</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search Engines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual Materials</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shareware/Freeware</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Social Networking (NEW)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software/Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam URLs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sports</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spyware/Adware</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Stock Trading</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Streaming Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Technical Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical/Business Forums</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Text Translators (NEW)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Text/Spoken Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tobacco</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Usenet News</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Violence</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Visual Search Engine</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Weapons</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web Ads</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Web Mail</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web Meetings (NEW)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web Phone</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Configuring an exempting action

An exemption is recommended as action for some categories in the previous section.

The problem of exempting a category arises when a URL falls into multiple overlapping categories and one category is set to Block and another to Allow. By default, the Block action takes precedence, and the URL will be blocked. There are, however, occasions when you may want to let the Allow action override the Block action, in which case you will “exempt” the category you want to allow.

For example, the URL for OhioStateAlumni.org might be categorized under both Education/Reference and Dating/Social Networking because there are portions of the site that relate to social and professional networks. If a school has the category of Education/Reference allowed, but the category of Dating/Social Networking blocked, then the entire site will be blocked.

In order to exclude URLs with overlapping categories from getting blocked, you must “exempt” the Education/Reference Category.

An action like this is not included in the built-in actions provided by McAfee Web Gateway. So if you want to use it, you need to create it as a new action using the Action Editor.

You can create the action by duplicating the existing Allow action and configure a severity of 50 for it, which ensures the overriding of a Block action on conflicting occasions.

Proceed as follows:

1. In the user interface, go to Configuration > Action Editor.
2. From the drop-down list at the bottom of the Action Editor tab, select Allow as action.
3. Click Create New From Existing. This creates the duplicated AllowNew action, which is displayed in the actions list on the tab.
4. Click Edit next to the AllowNew action. This opens the Action Definition tab, where you can configure further settings for the new action.
5. In the Name of Action input field, type Exempt as new name of the action.
6. Click Apply Above Changes in the middle of the tab.
7. From the Parameter drop-down list at the bottom of the tab, select Severity and click Add. This takes you to the Action Parameter tab.
8. In the Severity input field of that tab, type 50, instead of the default 10.
9. Click Apply Changes And Go Back.

The new Exempt action has now been configured. It is included in all action lists within McAfee Web Gateway, so you can select it as category action for Education/Reference on the Category Actions tab, see the Category actions section.

Any URL that is included in this category is then allowed to pass even if an overlapping category for it is set to Block.
**Quotas and coaching**

The **Quotas and Coaching** options are invoked by clicking on the corresponding button under **URL Filter**. These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **URL Filtering Methods** button:

| Policy: |  
| --- | --- | 
| default | URL Filtering Methods | 

The options are described in the upcoming section:

- **Quotas and coaching**

**Quotas and coaching**

The **Quotas and Coaching** tab looks like this:

- **Time Quota Options** - Defines the amount of time users can access the Web
  - 30 minutes per day
  - 150 minutes per week
  - 500 minutes per month

- **Count Volume Quotas** - Defines the amount of data a user can download from the Web
  - 5 MB per day
  - 30 MB per week
  - 100 MB per month

- **Session Length for Quotas** - Defines how long a user can access the Web at a time
  - 10 minutes

- **Session Length for Coaching** - Alerts users to time remaining for Web access
  - 2 minutes

There are four sections on this tab:

- **Time Quota Options**
- **Count Volume Quotas**
- **Session Length for Quotas**
- **Session Length for Coaching**
**Time Quota Options**

The **Time Quota Options** section looks like this:

<table>
<thead>
<tr>
<th>Time Quota Options</th>
<th>- Define the amount of time a user can access the Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 minutes per day</td>
<td>150 minutes per week</td>
</tr>
</tbody>
</table>

Using this section, you can configure quota to limit the time for Web access by users within your network. If a time quota has been configured, a notification page will be displayed to a user that accesses a Web site. This page contains the current usage information and the maximum amount of time allowed. The user has the choice of whether or not to continue access sites for the pre-configured amount of time.

After specifying the appropriate settings, click **Apply Changes** to make them effective. Use the following input fields to configure time quota:

- **. . . minutes per day** — Enter the time (in minutes) here that you want to allow per day.
- **. . . minutes per week** — Enter the time (in minutes) here that you want to allow per week.
- **. . . minutes per month** — Enter the time (in minutes) here that you want to allow per month.

**Count Volume Quotas**

The **Count Volume Quotas** section looks like this:

<table>
<thead>
<tr>
<th>Count Volume Quotas</th>
<th>- Defines the amount of data a user can download from the Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 MB per day</td>
<td>30 MB per week</td>
</tr>
</tbody>
</table>

Using this section, you can configure quota to limit the volume of Web access by users within your network. If a volume quota has been configured, a notification page will be displayed to a user that accesses a Web site. This page contains the current usage information and the maximum amount of volume allowed. The user has the choice of whether or not to continue access sites for the pre-configured amount of volume.

If you want to configure volume quota, select the checkbox next to the section heading. After specifying this setting and the other settings for volume quota, click **Apply Changes** to make them effective.

Use the following input fields to configure volume quota:

- **. . . minutes per day** — Enter the volume (in MB) here that you want to allow per day.
- **. . . minutes per week** — Enter the volume (in MB) here that you want to allow per week.
- **. . . minutes per month** — Enter the volume (in MB) here that you want to allow per month.

**Session Length for Quotas**

The **Session Length for Quotas** section looks like this:

<table>
<thead>
<tr>
<th>Session Length for Quotas</th>
<th>- Define how long a user can access the Web at a time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 minutes</td>
<td></td>
</tr>
</tbody>
</table>

Using this section, you can configure a limit to the time of Web access by users within your network. This limit will apply to those sites that time or volume quota have been configured for.

A warning will be displayed to a user when the time limit is shortly before being reached. The user has the choice to continue or not access to the site in question.
After specifying the appropriate setting, click **Apply Changes** to make it effective.

Use the following input field to configure the session length for quotas:

- **... minutes** — Enter the number of minutes you want to allow for this session length here. The default time is 10 minutes.

### Session Length for Coaching

The **Session Length for Coaching** section looks like this:

![Session Length for Coaching](image)

Using this section, you can configure a limit to the time of Web access by users within your network. This limit will apply to those sites that coaching has been configured for.

A warning will be displayed to a user when the time limit is shortly before being reached. The user has the choice to continue or not access to the site in question.

After specifying the appropriate setting, click **Apply Changes** to make it effective.

Use the following input field to configure the session length for coaching:

- **... minutes** — Enter the number of minutes you want to allow for this session length here. The default time is 2 minutes.

### Filter by expressions

The **Filter by Expressions** options are invoked by clicking on the corresponding button under **URL Filter**.

If you want to enable any of these options, make sure the checkbox on this button is also selected. The checkbox is selected by default.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **URL Filtering Methods** button:

![Policy and URL Filtering Methods](image)

The options are described in the upcoming section:

- **Filter by expressions**
Filter by expressions

The Filter by Expressions tab looks like this:

There are two sections on this tab:
- Filter by Expressions
- Expression List

Filter by Expressions

The Filter by Expressions section looks like this:

Using this section, you can configure the action that should be executed if one of the shell expressions entered in the Expression List is found in a URL.

Furthermore, you can enable the filtering of URLs based on their parameters. This will apply, however, only to GET parameters. These are parameters that are used for retrieving information. They include the request header and the URL name.

After specifying the appropriate settings, click Apply Changes to make them effective.

Use the following items to configure filtering by expressions:
- Matching shell expression — From the drop-down list labeled this way, select an action that should be executed if the filtering-by-expressions filter matches.
• **Also scan parameter and request body** — Select this checkbox to have URLs also scanned based on their parameters.

  **Note:** This setting applies to GET parameters only.

### Expression List

The **Expression List** section looks like this:

This section displays a list of the shell expressions that were configured in the **Filter by Expressions** section for URL filtering. Using this section, you can add expressions to the list and edit or delete them.

To add an expression, use the area labeled:

• **Add new shell expression** — Select **String** or **International Domain Name** from the first of the drop-down lists provided here.

  In the input field next to it, enter a string to specify the object using shell expressions.

  Select **International Domain Name** if you want to enter non-ASCII characters and the string should be used for the domain part of an URL.

  In some countries like Germany, Sweden, or Japan, domain names with non-ASCII characters are allowed.

  The IDNA (International Domain Names in Applications) standard describes how a Web browser should convert such a domain name into pure ASCII notation used, such as by DNS.

  Webwasher uses the pure ASCII notation as well; therefore, all IDN strings must be converted. This is done automatically when you select **International Domain Name** and enter a string with non-ASCII characters.

  **Note:** You can not use shell expressions with IDN strings.

Furthermore, use the following items when adding a new entry to the list:

• **Description** — Enter a text describing the shell expression in this input field. Input in this field is optional.

• **deactivate** — Enable this option to insert a new URL in the list that will, however, not yet be used for filtering.

• **allow matching URL** — Enable this option to exclude the URL you are about to enter from filtering.

• **ignore matching parameter** — Enable this option to skip parameters and apply all enabled filters, even if no match is found.
This option is only available if the **Also scan parameter and request body** option in the **Filter by Expressions** section on this tab is enabled.

- **Add** — After specifying the information for an expression, click this button to add it to the list.
  
  This addition will be valid only under the policy you are currently configuring.
  
  To add an expression to the list for all policies, select **Add to all policies** before clicking on the button.
  
  If a shell expression that was configured under another policy is already in the list, the setting of the **Add to all policies** checkbox will have no effect.

The **Expression List** is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled **Number of entries per page** and enter it using the **Enter** key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the corresponding input field and select or deselect the **deactivate**, **allow matching URL**, and **ignore matching parameter** checkboxes in the same line.

Then click **Apply Changes** to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- **Filter** — Type a filtering term in the input field of the **Expression** or **Description** column or in both and enter this using the **Enter** key of your keyboard. The list will then display only entries matching the filter.

- **Delete Selected** — Select the entry you wish to delete by selecting the **Select** checkbox next to it and click this button. You can delete more than one entry in one go. To delete all entries, select the **Select all** checkbox and click this button.

### Web reputation

The **Web Reputation** options are invoked by clicking on the corresponding button under **URL Filter**.

If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

These are policy-dependent options, they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled **Policy**, which is located above the **URL Filtering Methods** button:

```plaintext
Policy:
- [ ] default
- [ ] URL Filtering Methods
```

The options are described in the upcoming section:

- **Web reputation**
Web reputation

The **Web Reputation** tab looks like this:

There is the following section on this tab:

- **Web Reputation**

Web Reputation

Using this section, you can configure actions, such as Allow, Block, Block & Log Reputation, and others, that will be executed for Web resources with a given reputation.

Resources (URLs) are assigned reputation scores within McAfee Web Gateway, indicating to what degree they can be trusted. These scores can take values on a scale from -127 to +127 and are provided by the TrustedSource Web Database, where a huge amount of data has been collected on millions of URLs.

You can configure different actions for resources with a good, neutral or bad Web reputation. A bad reputation means that the URL in question is probably malicious, whereas a good reputation means that it is trustworthy.

Invoking a malicious URL means that you are putting your system or its content at risk by going to the corresponding Web site. This is usually due to something malicious, which may be a virus, spyware, phishing, etc., but could also be due to something illegal about where you are going.

Furthermore, you can configure what counts as good, neutral or bad reputation by setting threshold values for separating neutral from bad, as well as good from neutral reputation.

**Note:** Under the system applied here, high reputation scores are associated with bad reputation and low or even negative scores with neutral and good reputation.

Webwasher classifies URLs according to their reputation scores, using five different degrees, which are **Malicious** (50 or more), **Suspicious** (30 to 49), **Unverified** (15 to 29), **Neutral** (0 to 14), and **Trusted** (below zero). For more information on the meaning of each degree, see the Web reputation subsection of the Quick snapshot section.
The number of URLs that were processed by the McAfee Web Gateway URL Filter for each of these degrees is displayed in the diagrams on the Web Reputation tab under URL Filter > Quick Snapshot. After modifying the settings in this section, click Apply Changes to make the modification effective.

Use the following input fields and drop-down lists to configure Web reputation actions:

- **Action if Web reputation is "Bad"** — From this drop-down list, select an action for URLs with a bad Web reputation. The default action is Block and Log Reputation.

- **Neutral/Bad Threshold (input number between –127 and +127)** — In this input field, enter a value for the reputation score that should be the threshold for separating neutral from bad reputation. The default value is 14.

- **Action if Web reputation is "Neutral"** — From this drop-down list, select an action for URLs with a neutral Web reputation. The default action is Log Reputation.

- **Good/Neutral Threshold (input number between –127 and +127)** — In this input field, enter a value for the reputation score that should be the threshold for separating good from neutral reputation. The default value is 0.

- **Action if Web reputation is "Good"** — From this drop-down list, select an action for URLs with a good Web reputation. The default action is Allow.

### Extended List Manager

The Extended List Manager options are invoked by clicking on the corresponding button under URL Filter. They are described in the upcoming section:

- **Extended List Manager**
**Extended List Manager**

The **Extended List Manager** tab looks like this:

There are four sections on this tab:

- **Current Status**
- **Export**
- **Import**
- **Extended List**

**Current Status**

The **Current Status** section looks like this:

This section displays the number of Extended List entries that are currently loaded into memory. The default file name is `wwextendedlist.txt`.
URL Filter
Extended List Manager

If you want to use a different file name, enter this name (not including the path) in the input field provided here and click **Reload Into Memory**. The file will be stored in the `conf/dynablocator` directory.

**Export**

The **Export** section looks like this:

- **Export** - Retrieves the currently used Extended List file
  - Show file content in Web browser
  - Save file to disk
  - Export

Using this section, you can view the Extended List that is currently being used in a Web browser. You can also save the corresponding file to disk by clicking **Export**.

**Import**

The **Import** section looks like this:

- **Import** - Transfers an Extended List file to Webmaster
  - [ ] Immediately load into memory

Using this section, you can import an Extended List to McAfee Web Gateway. You can either immediately load the corresponding file into memory, which is the default option or browse for it and load it into memory later.

**Extended List**

The **Extended List** section looks like this:

- **Extended List** - Adds new Extended List entry
  - Add URL: <url>
  - Select one or more categories for the above URL:
    - Category 1: Please select
    - Category 2: Please select
    - Category 3: Please select
  - [ ] Use categorization for all subhosts

Using this section, you can add URLs to the Extended List and categorize them within that list.

**Note:** The number of URLs you can add to the list is not unlimited. A tool is provided for handling problems that may occur when adding entries to the list.

For more information about this tool, please contact the McAfee Technical Support team.

To add a URL, enter it in the input field provided here. Then select one or up to three categories from the drop-down lists below.

After specifying these settings, click **Add** to add the URL to the list.

You can also distribute this categorization to all subhosts in a cluster. If you want to use this option, make sure the corresponding checkbox in this section is selected. The checkbox is selected by default.

After modifying this setting, click **Apply Changes** to make the modification effective.
Category scheme

The **Category Scheme** options are invoked by clicking on the corresponding button under **URL Filter**. They are described in the upcoming section:

- **Category scheme**

## Category scheme

The **Category Scheme** tab looks like this:

![Category Scheme Tab](image)

There is the following section on this tab:

- **Category Scheme**

### Category Scheme

This section shows whether an upgrade has been performed from using a former Webwasher scheme of URL categories to the TrustedSource Web Database list of categories. This list is here referred to as SmartFilter category scheme, as it is also used by the McAfee SmartFilter product.

If this upgrade has not yet been performed, the section allows you to do it.

For more information about the versions of the former Webwasher software that required an upgrade, see the **Category actions** section.
When an upgrade to the TrustedSource Web Database list of categories has not yet performed, the section looks like this:

- **Category Scheme** - Upgrade to SmartFilter category scheme

  [Upgrade](#) to SmartFilter category scheme. By upgrading to the SmartFilter category scheme, you can review and fine-tune the policy after the upgrade. Attention: The upgrade process must be completed before performing the upgrade.

You need to restart McAfee Web Gateway after the upgrade to make it effective, and the upgrade cannot be undone. For this reason, it is recommended that you backup your configuration before performing the upgrade.

On the **Category Actions** tab, there is also an alert to make you aware of the upgrade option, in case you have not yet upgraded:

- You are using the Webwasher category scheme. An [upgrade to the SmartFilter category scheme](#) is available.

You can use the link that is displayed with the alert to go to this tab here, where the following items are provided for performing the upgrade:

- **backup your configuration** — Click this link to go to the **Configuration** tab under **Configuration > Backup & Restore**. Use the items provided on this tab to backup your configuration. Then return to the **Category Scheme** tab to continue with the upgrade procedure.

- **Upgrade** — Click this button to perform an upgrade from the old Webwasher category scheme to the TrustedSource Web Database list of categories. Then restart McAfee Web Gateway to make the upgrade effective.

  **Note**: The filter policies you configured under the old Webwasher version will be migrated during the upgrade. After performing the upgrade, you can review these policies if you wish to do so.

---

**Progressive lockout**

The **Progressive Lockout** options are invoked by clicking on the corresponding button under **URL Filter**.

If you want to enable any of these options, select the checkbox that is on this button. Then click **Apply Changes** to make this setting effective.

The options are described in the upcoming section:

- **Progressive lockout**
Progressive lockout

The Progressive Lockout tab looks like this:

There is the following section on this tab:

- **Progressive Lockout**

**Progressive Lockout**

Using this section, you can view the Progressive Lockout List. This is a list of the clients that are currently locked out. You can unlock clients that are on this list and also reset them to the never locked-out status.

Clients are locked out after sending a given number of requests that triggered a blocking action with a lockout parameter. A lockout parameter can be configured with any action, but is meaningful only with blocking actions.

If an action is configured with this parameter, a client-specific counter is increased by McAfee Web Gateway every time the action is triggered for a request by the client in question. After reaching a given value, the client is locked out for a given number of seconds.

The lockout interval is usually configured to increase with every time that a lockout is imposed on a client (progressive lockout). The interval can be reset, however, to its initial value.

**Note:** An action that has been configured with a lockout parameter is executed as usual whenever it applies. This means that a client would be blocked by a blocking action after requesting a URL of a particular category, regardless of whether this has already occurred often enough to impose also a lockout on the client.

The following information is provided on the Progressive Lockout List for every client that was locked out:

- **User Identifier** — ID for identifying a client. This is the ID that the client is also identified by on the Welcome Page.

- **Locked Out Until** — Date and time when the lockout interval finishes

- **Lock Count** — Number of times that the client has been locked out so far.
Use the following items to perform various activities relating to the list:

- **Filter** — Type a filtering term in this input field and enter it using the Enter key of your keyboard. The list will then display only client entries matching the filter.

- **Unlock Selected** — Select the client you wish to unlock by select the Select checkbox next to it and click this button. You can unlock more than one client at a time. To unlock all clients, select the Select all checkbox and click this button.

- **Reset Selected** — Select the client you wish to reset to the never-locked-out status by selecting the Select checkbox next to it and click this button. This means that the lockout interval will again have its initial value next time. You can reset more than one client at a time. To reset all clients, select the Select all checkbox and click this button.

---

**GTI settings**

The **GTI Settings** options are invoked by clicking on the corresponding button under **URL Filter**.

The options are described in the upcoming section:

- **GTI settings**

**GTI settings**

The **GTI Settings** tab looks like this:

<table>
<thead>
<tr>
<th>GTI Settings</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In-the-Cloud Rating</strong></td>
<td>?</td>
</tr>
<tr>
<td>- Disabled</td>
<td></td>
</tr>
<tr>
<td>- Always used</td>
<td></td>
</tr>
<tr>
<td>- Used if local rating yields no result</td>
<td></td>
</tr>
<tr>
<td><strong>Cloud Server Settings</strong></td>
<td>?</td>
</tr>
<tr>
<td>- Use default cloud server</td>
<td></td>
</tr>
<tr>
<td>- Use specific cloud server (name:port):</td>
<td>80</td>
</tr>
<tr>
<td><strong>Lookup Timeout Settings</strong></td>
<td>?</td>
</tr>
<tr>
<td>- Treat timeout as categorization error</td>
<td></td>
</tr>
<tr>
<td>- Cloud lookup timeout: 2000 (msec)</td>
<td></td>
</tr>
</tbody>
</table>

There are three sections on this tab:

- **In-the-Cloud Rating**
- **Cloud Server Settings**
- **Lookup Timeout Settings**
**In-the-Cloud Rating**

Using this section, you can configure where information to rate a URL is retrieved from.

Rating information includes information on the categories a URL belongs to, for example, *Online Shopping* or *Travel*, as well as the web reputation score. The information can be retrieved by looking it up “in the cloud”, which means that McAfee Web Gateway connects to the Global Threat Intelligence (GTI) system to retrieve the information.

This system is maintained by McAfee to provide information on categories and reputation scores for URLs, based on the content of the corresponding web pages. Various technologies, such as link crawlers, security forensics, honeypot networks, sophisticated auto-rating tools, and customer-submitted data are used to gather this information. An international, multi-lingual team of McAfee web analysts evaluates the information and enters URLs under particular categories into a database. To gather information on the reputation of a URL, its behavior on a worldwide real-time basis is analyzed, for example, where a URL shows up in the web, its domain behavior, and other details.

Information retrieved from this system is also stored in an internal database and can be retrieved through a local lookup. You can also configure both ways of looking up rating information in a way that in-the-cloud information is only looked up if a local lookup yields no results.

After specifying these settings, click **Apply Changes** to make them effective.

Use the following radio buttons to configure the lookup for URL rating information:

- **Disabled** — When selected, no URL rating information is looked up in-the-cloud.
- **Always used** — When selected, URL rating information is always looked up in-the-cloud.
- **Used if local rating yields no result** — When selected, URL rating information is only looked up in-the-cloud if a local lookup was performed before, but yielded no results.

**Cloud Server Settings**

Using this section, you can configure which server McAfee Web Gateway should connect to when using the Global Threat Intelligence (GTI) system to look up URL rating information “in the cloud”.

This server can be a default server or a server that you choose by specifying its name and a port number.

After specifying these settings, click **Apply Changes** to make them effective.

Use the following radio buttons and input field to configure a server for the in-the-cloud lookup:

- **Use default cloud server** — When selected, the default server is used for the in-the-cloud lookup.
- **Use specific cloud server** — If you do not want to use the default server, enter the name of the server you want to use instead in the first part of the input field provided here. In the second part enter a port number.

  *Note:* The default port number is 80.

**Lookup Timeout Settings**

Using this section, you can configure the way a timeout is handled by McAfee Web Gateway when it occurs during a lookup for URL rating information in the Global Threat Intelligence (GTI) system.

A timeout can, for example, occur if McAfee Web Gateway cannot connect to the GTI server in time.

After specifying these settings, click **Apply Changes** to make them effective.

Use the following checkbox and input field to configure timeout handling:

- **Treat timeout as categorization error** — When selected, a timeout during the lookup for URL rating information is treated as a categorization error.

  The URL is then considered as uncategorized. The action that has been configured in the Default Action section of the URL Filtering Methods tab is executed.

  Otherwise, the timeout is not treated as a categorization error, although the URL is not categorized. The action that has been configured in the Default Action section of the URL Filter Methods tab is not executed.
If a timeout is treated as a categorization error, an entry for the timeout can be written into the errors.log file. To have such entries written, you need to set a parameter in the global configuration file, which is the global.ini file under a Microsoft Windows operating system and the global.conf file under Linux.

In the global configuration file, go to the AccessControl section and set:

CloudDebugTimeout=1

In the errors.log file, you will then see entries reporting categorization errors due to timeouts in the following way:

Timeout during cloud lookup for URL <URL name>

- **Cloud lookup timeout** — In this input field, enter a value for the lookup timeout (in milliseconds).