# Dr.WEB®
for MIMEsweeper

Defend what you create

Administrator Manual

TRADEMARKS
Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web for MIMEsweeper
Version 6.0.1
Administrator Manual
07.02.2013

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1. Introduction

Thank you for purchasing **Dr.Web for MIMEsweeper**. This product is a plug-in for ClearSwift MIMEsweeper for SMTP designed to protect corporate mail systems against viruses and spam.

With the use of **Dr.Web for MIMEsweeper**, the ClearSwift content scanner incorporates the latest and most advanced anti-virus technologies of **Doctor Web** aimed to detect and neutralize the malicious objects which may present a threat to mail servers operation and information security. If you purchased the plug-in with the «Anti-virus&Anti-spam» license (and an appropriate license key file), it also identifies unsolicited e-mail messages using the VadeRetro spam filter.

Dr.Web for MIMEsweeper checks all e-mail messages received by the content filter for viruses, dialer programs, adware, riskware, hacktools and joke programs. If the plug-in is licensed to operate in the Anti-virus&Anti-spam mode, it also identifies unsolicited e-mails. On detection of a security threat, the plug-in classifies the infected or unsolicited messages according to the ClearSwift MIMEsweeper policies and neutralizes the malicious objects.

Main Features

Dr.Web for MIMEsweeper plug-in:

- Protects you from viruses in e-mails including malicious objects in archived attachments
- Detects malware
- Recovers infected objects
- Detects spam using VadeRetro technology
- Performs the checks fast and efficiently
- Automatically updates virus databases and plug-in components

This guide helps administrators to install and configure **Dr.Web for MIMEsweeper** to work with ClearSwift MIMEsweeper for SMTP.

For detailed information on the content filter scenarios, refer to the ClearSwift official web site at http://www.clearswift.com/products/msw/smtp/eval/avscenario.aspx.

Conventions

This guide utilizes the following content conventions and signs (see Table 1).

Table 1. Document Conventions and Signs

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of **Dr.Web** products and components.
Green and underlined	Hyperlinks to topics and web pages.
`Monospace`	Code examples, input to the command line and application output.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign ('+')	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
⚠	A warning about potential errors or any other important comment.

Contacting Support

Support is available to customers who have purchased a commercial version of **Doctor Web** products. Visit **Doctor Web Technical Support** web site at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in Dr.Web knowledge database at http://wiki.drweb.com/
- Browse the Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, see the **Doctor Web** official web site at http://company.drweb.com/contacts/moscow.

Chapter 2. Licensing

The use rights for the product are regulated by the *license key* file.

License Key File

The license key has the .key extension and contains, among other, the following information:

- Licensed period for the product
- Permission to use the VadeRetro spam filter
- Users number limitation for the license

A *valid* license key file satisfies the following criteria:

- License is not expired
- License applies to all components of the product
- License extends for use on mail servers
- Integrity of the license key file is not violated

If any of the conditions are violated, the license key file becomes *invalid*, **Dr.Web for MIMEsweeper** stops detecting and neutralizing malicious programs and transmits the messages unchanged. License violation is registered in the Windows Event Log.

See Logging for detailed information on events.

Acquire License Key Files

You can receive a license key file in one of the following ways:

- By e-mail in an archived attachment
- With the plug-in distribution kit
- On separate media

To acquire a license key file by e-mail

1. Launch an Internet browser and go to the site specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number which is typed on the registration card.
4. The license key file is archived and sent to the e-mail address you specified in the registration form. Extract the license key file and copy it to the program installation folder (usually, %ProgramFiles%\DrWeb for MIMEsweeper). Windows operating systems extract files from ZIP-archives automatically. You do not need to purchase or install additional software.

For demonstrative purposes **Doctor Web** may provide you with a *trial license key file*. Trial license allows you to access full functionality of the plug-in for a short-term period. No support is provided during trial period. On the expiration of the trial license, you will need to purchase a full license to continue working with the product.

To receive a trial license key file by e-mail, fill in the registration form at http://download.drweb.com/demoreq/.

Update License

When license expires or security of your system is reinforced, you may need to update the license. The new license then should be registered with the product. **Dr.Web for MIMEsweeper** supports hot license update without stopping or reinstalling the plug-in.

To update the license key file

1. Replace an old license key file with the new file in the program installation folder (usually, %ProgramFiles%\DrWeb for MIMEsweeper) or user-defined folder. The name of the new license key file must be the same as the name of the old license key file.
2. **Dr.Web for MIMEsweeper** automatically switches to the new license.

For more information on license types, visit the **Doctor Web** official web site at http://www.drweb.com.

Use License Key Files

By default, the license key file should be located in the program installation folder (usually, %ProgramFiles%\DrWeb for MIMEsweeper). The plug-in verifies the file regularly. Do not edit or otherwise modify the file to prevent the license from compromise.

Installation wizard copies and registers the license key file to the program installation folder. When installation completes, you can change location of the license key file.

To change license key file location

This operation is recommended for experienced users only. Serious problems might occur if you modify the registry incorrectly. Microsoft recommends to backup the registry before you modify it.

1. Open a registry editor.
2. Navigate to

   HKEY_LOCAL_MACHINE\SOFTWARE\DOCTOR WEB\DRWEB FOR MIMESWEEPER\LICENSE.

3. Right click the FILE key and select **Modify**.
4. Enter the path to the license key file.
5. Click **OK** and close the registry editor.
6. To restart **Dr.Web for MIMEsweeper**, open MIMEsweeper for SMTP Policy Editor and on the toolbar click **Save MIMEsweeper Policy** .

Dr.Web for MIMEsweeper is ready to use the license key file located in the selected folder.

Licensing Parameters

The license key file regulates the use of **Dr.Web for MIMEsweeper**.

The license key file is secured with digital signature. Do not edit or otherwise modify the file to prevent the license from compromise.

To view license details

1. View the license key file (for instance, open the file with the Notepad text editor.)
2. Review the following licensing parameters (see Table 2).

Table 2. Licensing Parameters

Parameter	Description
`[Key] | Applications`	Determines the application components licensed with the key.
`[Key] | Expires`	Determines the license expiration date.
`[User] | Name`	Determines the license owner.
`[Settings] | MailServer`	Determines if the license can be used on mail servers.
`[Settings] | SpamFilter`	Determines if the VadeRetro spam filter is licensed with the key. The spam filter is available for «Anti-virus&Anti-spam» licenses only.
`[Settings] | EmailAddresses`	Determines the number of users which the plug-in is licensed to protect simultaneously.

3. Close the file without saving.

Chapter 3. Installation

Dr.Web for MIMEsweeper resides on computers where the ClearSwift MIMEsweeper for SMTP is installed. It operates as a type 1 content filter scenario which is recommended by the ClearSwift company for the anti-virus software.

For more information on content scanner scenarios, refer to the ClearSwift official web site at http://www.clearswift.com/products/msw/smtp/eval/avscenario.aspx.

System Requirements

Dr.Web for MIMEsweeper resides on computers where the content filter is installed and operates successfully if the computer meets the ClearSwift MIMEsweeper for SMTP requirements. Before beginning installation, review the following system requirements (see Table 3).

Table 3. System Requirements

Component	Requirement
Disk Space	Minimum 60MB of disk space for full installation.
Operating System	One of the following: • Microsoft® Windows® 2000 (Professional Edition, Server, Advanced Server or Datacenter Server) with SP4 and Update Rollup 1 • Microsoft® Windows Server® 2003 (Standard Edition, Enterprise Edition or Datacenter Edition) • Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition or Datacenter Edition) • Microsoft® Windows Server® 2008 R2 32- and 64-bit versions of the operating systems are supported.
Content Filter	ClearSwift MIMEsweeper™ for SMTP 5.2 of later.

Component	Requirement
Other	Internet connection to update virus databases and program components.

This section reflects requirements for **Dr.Web for MIMEsweeper** only. Refer to ClearSwift guides for content filter requirements.

Install Program

Before beginning installation, review the system requirements.

⚠ To install **Dr.Web for MIMEsweeper** you must have the Administrator privileges.

Single Policy Server Environment

To install the program

1. Copy the following files to the computer where ClearSwift MIMEsweeper for SMTP resides:
   - **drweb-mimesweeper-600-windows-nt.exe** installation package,
   - license key file.
2. Double-click **drweb-mimesweeper-600-windows-nt.exe** to open the Dr.Web for MIMEsweeper InstallShield Wizard.
3. On the **Welcome to the InstallShield Wizard for Dr.Web for MIMEsweeper** page, click **Next**.
4. On the **License Agreement** page, read the Dr.Web for MIMEsweeper License Agreement, select **I accept the terms of the license agreement** and click **Next**.
5. On the **Dr.Web key file** page, enter the path to the license key file or click **Browse** to select the file.

You need a valid license key file to complete installation and run **Dr.Web for MIMEsweeper**. To acquire the license key file from the **Doctor Web** official web site, click **Get key file**.

After you make selection, click **Next**.

6. If your computer connects to the Internet via proxy, on the **Dr.Web Updater Proxy Configuration** page select **Use Proxy** and enter the following information:

Field	Description
Proxy IP-address	Enter proxy-server name in the following format: *<address>*:*<port>* where *<address>* is the proxy server name or IP-address, *<port>* is the port the prosy-server uses.
User name, Password	If required, enter username and password for the Updater to use to connect to the proxy-server, or leave blank if proxy-server allows anonymous access.
Confirm Password	Confirm the password.

7. On the **Ready to Install the Program** page, click **Next** to start the installation.

   Installation wizard registers **Dr.Web for MIMEsweeper** and copies the license key file to the installation folder (usually, C:\Program Files\DrWeb for MIMEsweeper).

8. On the **Restart MIMEsweeper services** page, select restart option for the content filter services.
9. On the **InstallShield Wizard Completed** page, click **Finish**.

The content filter registers the plug-in only after the MIMEsweeper for SMTP Security Service is restarted.

This completes the installation of **Dr.Web for MIMEsweeper**. You need to configure ClearSwift MIMEsweeper for SMTP to use the plug-in.

Multiple Policy Servers Environment

If you use several ClearSwift MIMEsweeper for SMTP Policy Servers, then you need to install **Dr.Web for MIMEsweeper** to every computer where a Policy Server resides. The ClearSwift MIMEsweeper for SMTP scenarios apply to all Policy Servers. When you create a Content Scanner scenario which uses **Dr.Web for MIMEsweeper**, the Policy Server attempts to connect to the plug-in. If the plug-in is not installed on the computer where the Policy Server resides, the ClearSwift MIMEsweeper for SMTP cannot process the mail.

To install the program in multi-server environment

1. For each computer where the Policy Server resides, install the plug-in according to the installation instructions for the single policy server environment.
2. Repeat the step 1 for all computers where the Policy Server resides.

This completes the installation of **Dr.Web for MIMEsweeper**. You need to configure ClearSwift MIMEsweeper for SMTP to use the plug-in.

Uninstall Program

To uninstall **Dr.Web for MIMEsweeper** you must have the Administrator privileges.

To uninstall the program

1. Open MIMEsweeper for SMTP Policy Editor and navigate to the MIMEsweeper for SMTP Scenarios node (see Picture 1).
2. Right-click the plug-in scenario and select **Delete**.
3. At the prompt, click **Yes**.
4. On the toolbar, click **Save MIMEsweeper Policy** .
5. Exit MIMEsweeper for SMTP Policy Editor.

6. Use one of the following methods to access the program uninstall wizard:
   - On the Control Panel, double-click **Add or Remove Programs**, then in the programs list select **Dr.Web for MIMEsweeper** and click **Remove**.
   - Select **Start** -> **Programs** -> **Dr.Web for MIMEsweeper** -> **Uninstall Dr.Web for MIMEsweeper**.
7. At the prompt, click **Yes**. The uninstall wizard removes program files and update task.

The license key and log files are not deleted by default. You have to delete the files manually from the following folders:

- The license key file is located in the program installation folder (usually, %ProgramFiles%\DrWeb for MIMEsweeper) or user-defined folder.
- The plug-in logs are located in the Dr.Web logs folder (usually, %AllUserProfile%\Local Settings\Application Data\Doctor Web\Logs).

Configure Internet Connection for Updater

If the computer where the content filter resides connects to the Internet via proxy, you need to configure the Updater to connect to the proxy server.

To configure connection to a proxy-server

1. In the program installation folder (usually, %ProgramFiles%\DrWeb for MIMEsweeper), double-click UpdaterProxySetup.exe.
2. In the dialog window, select **Use Proxy**.
3. Enter the following information:

Field	**Description**
Proxy IP-address	Enter proxy-server name in the following format: *<address>***:***<port>* where *<address>* is the proxy server name or IP-address, *<port>* is the port the prosy-server uses.
User name, Password	If required, enter username and password for the Updater to use to connect to the proxy-server, or leave blank if proxy-server allows anonymous access.
Confirm Password	Confirm the password.

4. Click **OK**.

Chapter 4. Configuration

Dr.Web for MIMEsweeper resides on computers where the ClearSwift MIMEsweeper for SMTP is installed. It operates as a type 1 content filter scenario which is recommended by the ClearSwift company for the anti-virus software. If you purchased an «Anti-virus+Anti-spam» license, you can also enable spam check in addition to anti-virus protection.

To integrate the plug-in into the content filter

1. Open ClearSwift MIMEsweeper for SMTP Policy Editor.
2. Create a Dr.Web filtering scenario for e-mail messages.
3. Configure the Dr.Web filtering scenario.
4. If necessary, you can disable spam checks.

For more information on content scanner scenarios, refer to the ClearSwift official web site at http://www.clearswift.com/products/msw/smtp/eval/avscenario.aspx.

Create Content Scanner Scenario

ClearSwift MIMEsweeper for SMTP uses Content Scanner scenarios to scan content of e-mails using anti-virus software.

To create a content filtering scenario

1. Open ClearSwift MIMEsweeper for SMTP Policy Editor.
2. In the tree view, select **MIMEsweeper for SMTP | Policies**.

3. Right-click **Scenarios** and select **New | Content Scanner**.

   The New Content Scanner Wizard displays.

4. On the **Welcome to the Content Scanner Wizard** page, clear the **I want to create new items without using wizard option** and click **Next**.

5. On the **Initial Scenario State** page, select the following options:

Option	**Description**
Enabled	Turns on the scans for all received messages.
Overridable	Enables the scenario to be turned on or off in the subfolders (Incoming or Outcoming messages).

   Click **Next**.

6. On the **Scanner** page, select **Dr.Web for MIMEsweeper** in the list of anti-virus applications and click **Next**.
7. On the **Cleaning** page, select or clear the following options:

Option	**Description**
Clean the detected item	Select this option to cure infected messages with **Dr.Web for MIMEsweeper**. Clear this option to transmit messages without change.
Annotate the associated message	Select this option to add text notifications to cleaned messages. Clear this option to transmit messages without notification.

   Click **Next**.

8. On the **Stripping** page, select or clear the following options:

Option	**Description**
Strip the detected item	Select this option to delete malicious software. If this option is selected together with the Clean the detected item option, **Dr.Web for MIMEsweeper** attempts to cure infected objects first. Clear this option to transmit messages without change.
Annotate the associated message	Select this option to add text notification to stripped messages. Clear this option to transmit messages without notification.

Click **Next**.

9. On the **Classifications** page, configure messages classification. It is recommended to classify messages as follows:
   - For the **On detected items cleaned** option, select **Cleaned**. This labels the messages where infected objects are cured as Cleaned.
   - For the **On detected items stripped** option, select **Cleaned**. This labels the messages where infected objects are deleted as Cleaned.
   - For the **On threat cannot be removed** option, select **Virus**. This labels the messages with threats which **Dr.Web for MIMEsweeper** cannot cure as Virus.

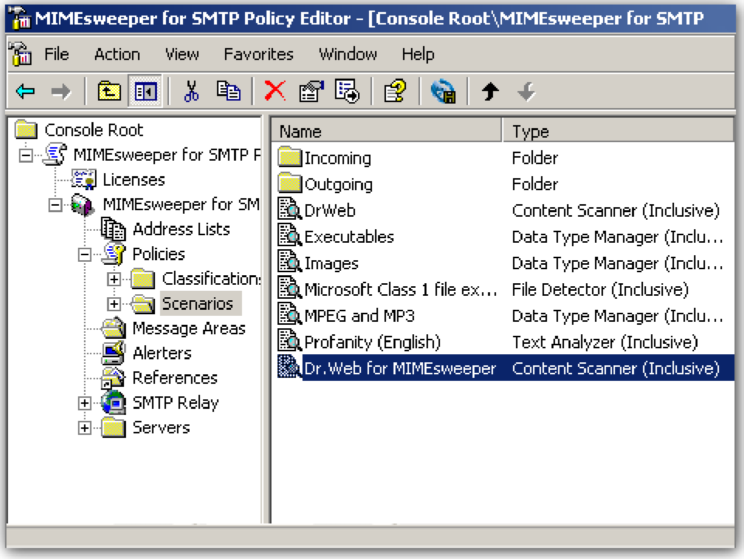
   Click **Next**.

10. On the **Scenario Name** page, enter the following information:

Field	Description
Name	Enter the name for the content filtering scenario.
Notes	Enter the brief description for the scenario.

Click **Next**.

11. On the **Completing the Content Scanner Wizard** page, review the scenario settings and click **Finish**.



Name	Type
Incoming	Folder
Outgoing	Folder
DrWeb	Content Scanner (Inclusive)
Executables	Data Type Manager (Inclu…
Images	Data Type Manager (Inclu…
Microsoft Class 1 file ex…	File Detector (Inclusive)
MPEG and MP3	Data Type Manager (Inclu…
Profanity (English)	Text Analyzer (Inclusive)
Dr.Web for MIMEsweeper	Content Scanner (Inclusive)

Picture 1. List of content filter scenarios

The Dr.Web scenario appears in the list of scenarios for ClearSwift MIMEsweeper for SMTP (see Picture 1).

Configure Content Scanner Scenario

To complete the configuration, you need to select data types which you want **Dr.Web for MIMEsweeper** to check.

To configure a content filtering scenario

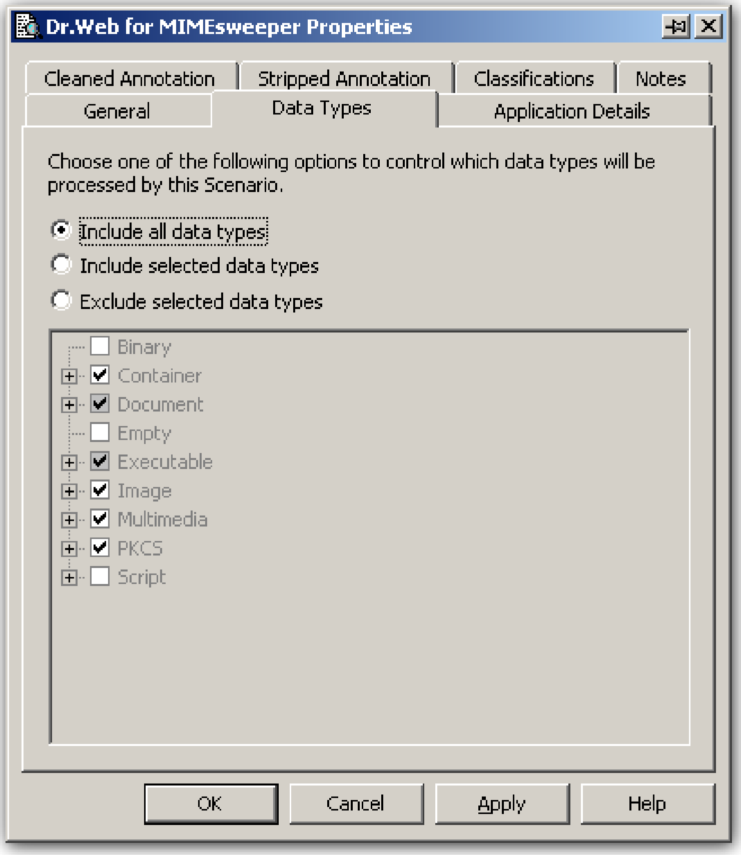
1. Open MIMEsweeper for SMTP Policy Editor and navigate to the MIMEsweeper for SMTP Scenarios node (see Picture 1).
2. Right-click the Dr.Web Content Scanner scenario and select **Properties**.

3. On the **Data Types** tab (see Picture 2), select one of the following options:
   - To check messages for viruses and spam, select **Include all data types**.
   - To scan messages for viruses only, select **Exclude selected data types**, then expand the **Containers** node and select **SMTP message**.
   - To detect spam messages only, select **Include selected data types**, then expand the **Containers** node and select **SMTP message**.

⚠ To separate infected messages from spam, you can create two Content Scanner Scenarios, then configure one of them to scan messages for viruses only and configure another one to scan messages for spam only.

4. If you selected **Annotate the associated message** on the **Cleaning** page of the New Content Scanner wizard, then select the **Cleaned Annotation** tab and configure the notification which you want to add to neutralized messages.
5. If you selected **Annotate the associated message** on the **Stripping** page of the New Content Scanner wizard, then select the **Stripped Annotation** tab and configure the notification which you want to add to messages stripped of infected objects.
6. Click **OK**.
7. In the list of scenarios for ClearSwift MIMEsweeper for SMTP, select the Dr.Web scenario and use the arrow ↑ on the toolbar to place the scenario at the top of the list. The content filter executes the scenarios in sequential order. To provide security, the anti-virus scenarios should be executed first.
8. On the toolbar, click **Save MIMEsweeper Policy**.

Dr.Web for MIMEsweeper is integrated into the ClearSwift MIMEsweeper for SMTP content filter.



Dr.Web for MIMEsweeper Properties

Choose one of the following options to control which data types will be processed by this Scenario.

● Include all data types

○ Include selected data types

○ Exclude selected data types

- □ Binary
- ☑ Container
- ☑ Document
- □ Empty
- ☑ Executable
- ☑ Image
- ☑ Multimedia
- ☑ PKCS
- □ Script

Picture 2. Data Types Tab

Disable Spam Checks

If necessary, you can disable spam check.

To disable spam checks

1. Open MIMEsweeper for SMTP Policy Editor and navigate to the MIMEsweeper for SMTP Scenarios node (see Picture 1).
2. Right-click the Dr.Web Content Scanner scenario and select **Properties**.
3. On the **Data Types** tab (see Picture 2), select **Exclude selected data types**, then expand the **Containers** node and clear the **SMTP message** option.
4. Click **OK**.
5. On the toolbar, select **Save MIMEsweeper Policy** .

Chapter 5. Checks

After you install **Dr.Web for MIMEsweeper**, it performs virus and spam checks on new mail messages transmitted through ClearSwift MIMEsweeper content filter. The messages stored on the server before plug-in was installed are not scanned.

Virus Checks

Dr.Web for MIMEsweeper checks new messages only. The messages stored on the server before plug-in was installed are not scanned.

Dr.Web for MIMEsweeper detects and neutralizes the following malicious objects:

- Viruses embedded in the mail message (Rich-Text or HTML format)
- Infected attachments including:
- Infected archives
- Infected mail messages
- Bomb viruses in files or archives
- Adware
- Hacktools
- Dialer programs
- Joke programs
- Riskware

Dr.Web for MIMEsweeper uses several detection methods to perform anti-virus checks on all e-mail messages transmitted via ClearSwift MIMEsweeper for SMTP. The infected messages are processed according to the Dr.Web Content Scanner scenario (see Table 4).

Table 4. Anti-virus scan settings

Setting	Description
Clean the detected item	If you select this option on the Cleaning page of the New Content Scanner wizard, **Dr.Web for MIMEsweeper** attempts to cure infected objects. Cured messages are marked according to the **On detected items cleaned** option which you select on the Classifications page of the New Content Scanner wizard.
Strip the detected item	If you select this option on the Stripping page of the New Content Scanner wizard, **Dr.Web for MIMEsweeper** deletes infected objects. If this option is selected together with the **Clean the detected item** option, the plug-in first attempts to cure infected objects. If an object cannot be cured, the plug-in deletes it. Only incurable objects are deleted. Messages with deleted objects are marked according to the **On detected items stripped** option which you select on the Classifications page of the New Content Scanner wizard.
Annotate the associated message	If you select this option on the Cleaning or Stripping pages of the New Content Scanner wizard, **Dr.Web for MIMEsweeper** adds a text notification to the message about the performed operations. The text depends on the message category and scenario settings.
On threat cannot be removed	If you select this option on the Classifications page of the New Content Scanner wizard, the messages with the threat which cannot be neutralized are marked according to the selected option. (The default is Virus.)

On detection, **Dr.Web for MIMEsweeper** attempts to cure infected objects, or deletes them if the cure option is not selected or the object cannot be cured. If the message has several attachments, only infected files are deleted. If the malicious code is embedded in the message body, the e-mail is moved to the quarantine. Clean messages, files and archives are transmitted without changes. Infected messages which the plug-in cannot neutralize are marked as viruses and moved to the quarantine. The content filter can also add to e-mails notifications or message headers to indicate actions performed by **Dr.Web for MIMEsweeper**.

Detection Methods

The **Doctor Web** anti-viruses simultaneously use several malware detection methods, which allow them to perform thorough checks on suspicious files and control software behaviour:

1. The scans begin with *signature analysis*, which is performed by comparison of file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Doctor Web** anti-viruses use signature checksums instead of using complete signature sequences. Checksums uniquely identify signatures which preserves correctness of virus detection and neutralization. The Dr.Web signature databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

2. On completion of signature analysis, the **Doctor Web** anti-viruses use the unique **Origins Tracing** method to detect new and modified viruses which use the known infection mechanisms. Thus the **Dr.Web** users are protected against such viruses as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the Origins Tracing mechanism allowed to considerably reduce the number of false triggering of the **Dr. Web** heuristics analyser.

3. The detection method used by the *heuristics analyser* is based on certain knowledge about attributes that characterize malicious code. Each attribute or characteristic has weight coefficient which determines the level of its severity and reliability. Depending on the sum weight of a file, the heuristics analyser calculates the probability of unknown virus infection. As any system of hypothesis testing under uncertainty, the heuristics analyser may commit type I or type II errors (omit viruses or raise false alarms).

While performing any of the abovementioned checks, the **Doctor Web** anti-viruses use the most recent information about known malicious software. As soon as experts of the **Doctor Web** virus laboratory discover new threats, the update for virus signatures, behaviour characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the **Dr.Web** resident guards and penetrates the system, then after update the virus is detected in the list of processes and neutralized.

Add Headers

You can add a notification text or message header to e-mails which will indicate actions performed by **Dr.Web for MIMEsweeper**. The information on performed action is stored in the MIMEsweeper Detected token. If the message is clean, the Detected token is empty. To distinguish dangerous messages from spam, which the content filter also marks as Virus, configure the content filter to add headers to infected messages which **Dr.Web for MIMEsweeper** cannot neutralize.

To add message headers

1. Open MIMEsweeper for SMTP Policy Editor and navigate to the MIMEsweeper for SMTP **Classifications** node under the **Policies** node.
2. Right-click the classification of e-mails for which you want to add a header, then select **New | Add Header**. This opens the New Add Header wizard.
3. On the **Welcome to the New Add Header Wizard** page, click **Next**.

4. On the **Header Details** page, enter the following information:

Field	Description
Header Name	Enter the name for the header.
Header Value	Click the arrow on the **Tokens** button and select **Detected**. **Dr.Web for MIMEsweeper** sets value of the Detected token to reflect the type of the threat which the message contains. For the spam messages, the value is set to SPAM. For the messages which the plug-in cannot neutralize, the value is set to VIRUS.

   Click **Next**.

5. On the **Action Name** page, review and change if necessary the action name and description, then click **Next**.
6. On the **Completing the Add Header Wizard** page, click **Finish**.
7. To add headers to messages before further processing, select the classification node, then in the right pane select the Add Header action and use the arrow ↑ on the toolbar to place the action at the top of the list.
8. On the toolbar, click **Save MIMEsweeper Policy** .

Spam Checks

Dr.Web for MIMEsweeper uses VadeRetro technology to detect unsolicited messages in the mail transmitted via ClearSwift MIMEsweeper for SMTP. The VadeRetro spam filter is supplied configured and needs no additional teaching. The plug-in performs spam checks according to the Dr.Web Content Scanner scenario (see Table 5).

Table 5. Spam Check Settings

Option	Description
Include all data types	If you select this option on the Data Types tab of the Dr.Web Content Scanner properties window (see Picture 2), the plug-in performs spam checks.
Exclude selected data types, Containers | SMTP message	If you select this option under the Containers node in the data types list on the Data Types tab of the Dr.Web Content Scanner properties window (see Picture 2), the plug-in does not perform spam checks.
On threat cannot be removed	If you select this option on the Classifications page of the New Content Scanner wizard, the spam messages detected using **Dr.Web for MIMEsweeper** are labeled according to the selected option. (The default is Virus.)

The content filter assigns the same classification to unsolicited messages and messages which **Dr.Web for MIMEsweeper** cannot neutralize. (The default classification is Virus.) Such messages are automatically moved to the quarantine. To differentiate spam messages and infected messages, you can add headers to messages before they are moved to the quarantine.

You can also completely disable spam checks.

Chapter 6. Update

The Updater component (DrWebUpW.exe) launches automatically after completing the plug-in installation. It updates the scanning engine (drweb32.dll), spam filter (vrcpp.dll), and virus databases (*. vdb).

Dr.Web for MIMEsweeper uses virus databases to detect malicious software. These databases contain details and signatures for all viruses and malicious programs known at the moment of **Dr.Web for MIMEsweeper** release. However modern computer viruses are characterized by the high-speed evolvement and modification. More than that, within several days and sometimes hours, new viruses emerge which can infect millions of computers around the world. To mitigate the risk of infection during the licensed period, **Doctor Web** provides you with regular updates to virus databases and plug-in components. The Updater component of **Dr.Web for MIMEsweeper** helps you download the updates via Internet and automatically installs them.

When you install **Dr.Web for MIMEsweeper**, the installation wizard creates a task which schedules Updater to check for new updates at the **Doctor Web** global update server. You can change the schedule using the standard Windows Scheduled Tasks utility. You can also configure the update process using the command line parameters listed in the Appendix A.

For computers without access to the Internet, you can configure updates from the central storage of update files.

If your computer connects to the Internet via proxy, configure Updater to connect to the proxy-server.

To modify update schedule

1. On the Control Panel, double-click **Scheduled Tasks**.
2. Right-click **DrWeb for MIMEsweeper Update** and select **Properties**.
3. On the Schedule tab, modify the task schedule. By default, the plug-in checks for updates each 30 minutes.
4. Click **OK**.

To configure update without Internet connection

1. Create a central storage for the update files.

> You can use folder available through UNC paths only, which include:
>
> - Local folder on the computer
> - Shared network folders

2. Copy the new updates for the plug-in components and virus databases from the **Doctor Web** official download site at http://download.drweb.com/bases/ to the storage. You can view the list of updatable components in the drweb32.lst file which is located in the program installation folder (usually, %ProgramFiles&\DrWeb for MIMEsweeper).
3. On the local computer where you want to configure updates from the central storage, open the Control Panel and double-click Scheduled Tasks.
4. Right-click **Dr.Web for MIMEsweeper Update** and select **Properties**.
5. On the Task tab, add the following command line parameter to the command string in the **Run** field:

   /URL:<*storage*> where <*storage*> is the path to the central updates storage.

6. Click **OK**.

Updater is ready to download and install new files from the central storage without connecting to the Internet.

Chapter 7. Logging

Dr.Web for MIMEsweeper registers errors and application events in the following logs:

- Windows Event Log
- Text log

The text log is stored in the DRWMSWLog.log file in the %AllUserProfile%\Local Settings\Application Data\Doctor Web\Logs folder.

The update information is logged in a separate drwebupw.log file, which is located in the %AllUserProfile%\Application Data\Doctor Web\Logs\ folder.

Event Log

Dr.Web for MIMEsweeper registers the following information in the Windows Event Log:

- Plug-in starts and stops
- License key file parameters including validity, licensed period, and permission to use Anti-spam (Information is registered each time the plug-in checks the license or when the license file changes.)
- Parameters of the plug-in components including scanner, core, virus databases and Anti-spam if installed (Informational is registered when the plug-in starts or components are updated.)
- License invalidity notifications if the license key file is missing, some of the plug-in components are not licensed, license is blocked or license key file is corrupted (Information is registered when the plug-in checks the license.)
- License expiration notifications (A message is registered in 30, 15, 7, 3, 2 and 1 days before expiration.)

To view Event Log

1. On the Control Panel, double-click **Administrative Tools** and then double-click **Event Viewer**.
2. In the tree view, select **Application**.
3. The application Event Log displays in the right pane. The Source for the **Dr.Web for MIMEsweeper** events is **Dr.Web for MIMEsweeper**.

Text Log

Dr.Web for MIMEsweeper registers the following information in the text log (the DRWMSMLog file):

- License validity status
- Malware detection reports per each detected malicious object
- Spam detection reports
- Read or write errors
- Errors while scanning the archives or password-protected files
- Core failures
- License expiration notifications (A message is registered in 30, 15, 7, 3, 2 and 1 days before expiration.)

The text log file is cyclic. When the log size reaches the maximum (the default is 10 000 KB), **Dr.Web for MIMEsweeper** creates a new file and deletes the old one.

Chapter 8. Localization

Dr.Web for MIMEsweeper supports English (default) and Russian languages in user interface. Localization settings affect the UpdaterProxySetup.exe utility and log records only.

To change localization

> ⚠ This operation is recommended for experienced users only. Serious problems might occur if you modify the registry incorrectly. Microsoft recommends to backup the registry before you modify it.

1. Open a registry editor.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\DOCTOR WEB\DRWEB FOR MIMESWEEPER\LOCALE.
3. Right-click the LANGUAGE key and select **Modify**.
4. In the VALUE field, enter a standard language number:
   - To use Russian language, enter **1049**
   - To use English language, enter **1033**
5. Click **OK** and close the registry editor.
6. Restart **Dr.Web for MIMEsweeper**.

Chapter 9. Troubleshooting

If you experiencing trouble protecting you mail server from virus threats and spam, follow the steps below to ensure that **Dr.Web for MIMEsweeper** is installed and configured properly:

- Check installation
- Check Updater module
- Check integration with content filter

To check installation

1. Ensure that the plug-in created the following folders:
   - %ProgramFiles%\DrWeb for MIMEsweeper\
   - %CommonProgramFiles%\Doctor Web\
   - %AllUserProfile%\Application Data\Doctor Web\
2. On the Control Panel, double-click **Administrative Tools** and then double-click **Services**. Ensure that the following services are running:
   - Dr.Web Scanning Engine (DrWebEngine)
   - MIMEsweeper for SMTP Infrastructure
   - MIMEsweeper for SMTP Security Service
3. View Event Log and ensure that there is no errors which originate from **Dr.Web for MIMEsweeper**.
4. In the %AllUserProfile%\Local Settings\Application Data\Doctor Web\Logs folder, view the DRWMSWLog.log text log and ensure that is contains no errors.

To check Updater

1. On the Control Panel, double-click **Scheduled Tasks** and ensure that the **DrWeb for MIMEsweeper Update** task is created.
2. Check that last update succeeded. The program updates virus databases automatically after installation completes. If update completes successfully, the ERRORLEVEL environment variable is set to 0. Other values indicate an error.

3. In the %AllUserProfile%\Application Data\Doctor Web\Logs\ folder, view the DRWebUpw.log the update log and ensure that it contains no errors.

To check plug-in integration

1. Create and send an e-mail with the EICAR-Test-File in attachment to a mailbox on your mail server. For information on EICAR test virus refer to http://en.wikipedia.org/wiki/EICAR_test_file.
2. Check the received e-mail. If you configured the content filter according to this guide, the infected object must be cleaned or stripped. The message and its header may contain annotation which notifies you on the plug-in actions.
3. Send via SMTP to a mailbox on you mail server a spam message with the following text:

   ```
   Start enjoying the benefits of Generic Medic1ne. Order quickly and easily, and save a ton of money. Try them out, they're 100% m0ney back guarantee.
   ```

4. Check incoming messages. The content filter must move the message to quarantine directly without sending it to the address.

Appendices

Appendix A. Updater Command Line Parameters

The Updater can operate in command line mode. You can use parameters to configure the update process.

To configure update task

1. On the Control Panel, double-click **Scheduled Tasks**.
2. Right-click **DrWeb for MIMEsweeper Update** and select **Properties**.
3. In the **Run** field, add command line parameters.

Available Parameters

Below is the list of command line parameters which can be used to configure the updating process:

Parameter	Description
/DBG	Sets detailed logging in the %AllUserProfile%\Application Data\Doctor Web\Logs\drwebupw.log file.
/URL:*<url>*	Specifies location of the updates server. Only UNC-paths are accepted.
/USER: *<name>*	Specifies the user name to use when connecting to the updates server.
/PASS: *<password>*	Specifies the password to use when connecting to the updates server.

Parameter	Description
/UPM: *<mode>*	Configures connection via proxy. You can set one of the following values: • **direct** – direct connection without proxy, • **ieproxy** – connection via proxy, system settings are used, • **userproxy** – connection via proxy, user-defined settings are used.
/PURL: *<address>*	Specifies location of the proxy server.
/PUSER: *<name>*	Specifies the user name to use when connecting to the proxy server.
/PPASS: *<password>*	Specifies the password to use when connecting to the proxy server.
/UA	Sets the Update All mode when Updater downloads all files specified in the updating list regardless of the operating system used and the product components installed. This mode allows you to download all updates from the **Doctor Web** global update server. This mode cannot be used to update the anti-virus installed on a computer.
/ST	Sets the updater to run in stealth (invisible) mode.
/LNG: *<filename>*	Specifies the language resources file name. The default language is English.
/GO	Sets the package operation mode when Updater does not display dialogs.
/QU	Sets compulsory closure of Updater after finishing an update regardless of its results. Update result is returned in the ERRORLEVEL environment variable. If update completes successfully, the ERRORLEVEL environment variable is set to 0. Other values indicate an error.

Parameter	Description
/DIR: *<folder>*	Specifies the folder where to store the update files. The default is the directory where Updater runs.
/URM: *<mode>*	Sets the Restart mode. In this mode the computer is restarted when update finishes. You can set one of the following values: • **prompt** – prompt for reboot if needed, • **noprompt** – reboot without prompting if needed, • **force** – always reboot, • **disable** – disable reboot.
/REG	Launches Updater to register the product or request a license key file.
/UPD	Sets the Usual mode. Use this parameter together with **/REG** to update the product after completing registration.
/UVB	Sets update of virus databases and the core (drweb32.dll) only. This option disables **/UA** parameter.
/RP*<file>* or **/RP+***<file>*	Specifies the log file. The default is %AllUserProfile% \Application Data\Doctor Web\Logs\ drwebupw.log. Use **/RP+** to append new records to the file. Use **/RP** to overwrite the file.
/INI:*<path>*	Specifies an alternative configuration file to use.
/NI	Sets Updater to ignore parameters specified in the configuration file (drweb32.ini).
/NR	Sets Updater to work without logging.
/SO	Enables sound notifications on errors.

Index

Index

Index