Defend what you create

Administrator Manual

Dr.Web for IBM Lotus Domino for Linux
Version 6.00.2
Administrator manual
24.04.2013

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

Document Conventions and Abbreviations

Depending on the context, **Dr.Web** can mean either the name of the company – **Doctor Web**, or the name of the product – **Dr.Web for IBM Lotus Domino**.

The following conventions and symbols are used in this document:

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.
Exclamation mark	A warning about potential errors or any other important comment.

The following abbreviations are used in the manual:

- ACL - Access Control List;
- CPU - Central Processing Unit;
- GUI - Graphical User Interface;
- HTML - Hypertext Mark-up Language;
- HTTP - Hypertext Transfer Protocol;
- NSF - Notes Storage Facility (the file type for Lotus Notes and Lotus Domino databases);
- NTF - Notes Template Format (templates of NSF files);
- OS - operating system;
- RAM - Random Access Memory;
- SMTP - Simple Mail Transfer Protocol;
- UNC - Universal Naming Convention;
- URL - Uniform Resource Locator;
- VDB - Virus databases (files which contain virus signatures used by Dr.Web antivirus scanning engine);
- VGA - Video Graphics Array.

Chapter 1. Introduction

Thank you for purchasing **Dr.Web for IBM Lotus Domino**. It offers reliable protection from e-mail threats for computers and data inside a corporate network using the most advanced technologies.

This manual is intended to help administrators of large corporate networks to install, adjust and manage **Dr.Web for IBM Lotus Domino**.

What is Dr.Web for IBM Lotus Domino

Dr.Web for IBM Lotus Domino is a plug-in designed to assure anti-virus and anti-spam protection of the Lotus Domino system.

The structure of **Dr.Web for IBM Lotus Domino**, implementation of remarkable scanning methods and possibility to fully control the scanning process - all this accounts for high scanning speed and to a great extent spares system resources.

The anti-virus plug-in provides scanning of e-mail messages and documents in Lotus Domino server databases *on-the-fly* (in real time mode) or according to schedule. **Dr.Web for IBM Lotus Domino** isolates infected and suspicious documents by moving them to the **Quarantine**. Objects in the **Quarantine** and all the settings of the plug-in can be accessed via **Dr.Web Administrator Console** - a GUI which is run either via the Lotus Notes client or via a web browser (see Starting the Administrator Console). The updating utility can be launched either manually or according to schedule, which makes it easy to keep the virus databases and program files of the anti-virus package up to date.

Dr.Web for IBM Lotus Domino can perform the following functions:

- scan all incoming and outgoing messages in real time mode;
- scan documents in specified databases according to schedule;
- scan documents while working with them;
- scan scheduled replication traffic;
- scan cluster replication traffic;
- isolate infected and suspicious objects in the quarantine;
- filter and block spam with the possibility to manually compile black and white lists of addresses;
- group clients to simplify their management;
- send notifications on virus events and log them;
- distribute reports on virus and spam events;
- collect statistics;
- automatically update virus databases and components of the plug-in.

Dr.Web for IBM Lotus Domino uses virus databases which are constantly supplemented with new signatures to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.

Dr.Web for IBM Lotus Domino does not support the DB2 Universal Database (DB2 UDB) software.

Objects that are Scanned

Dr.Web for IBM Lotus Domino scans the following objects:

- files attached to e-mail messages;
- files attached to documents in databases;
- OLE objects.

Dr.Web for IBM Lotus Domino does not scan:

- encrypted messages;
- files created in OS/2 and Mac OS;
- local database replicas located on workstations.

License Key File

User's rights to use **Dr.Web for IBM Lotus Domino** are regulated by a special file called the *key file*. The key file contains the following information:

- duration of the anti-virus license
- list of components a user is allowed to use (e.g. the anti-spam feature can be enabled only in the "Anti-virus + Anti-spam" version)
- other restrictions (e.g. the number of users allowed to use the plug-in)

The key file has the **.key** extension and should be obtained before installing **Dr.Web for IBM Lotus Domino** as you will be asked to specify the path to your key file during installation.

For evaluation purposes you can use a demo key file, which can be received by filling out a web form on the official web site of **Doctor Web** (http://download.drweb.com/demoreq/?pid=82). The demo key file provides full functionality of the main anti-virus components, but has a limited term of usage.

To buy a license key file, you can use the **Doctor Web** web store service (http://buy.drweb.com/).

The key file is delivered as a file with the **.key** extension or as a ZIP archive containing such file.

The parameters of the key file which specify the user's rights are set in accordance with the License agreement. The file also contains information on the user and seller of the anti-virus.

The key file has a write-protected format and must not be edited. Editing the key file makes it invalid. Therefore, it is not recommended to open your key file with a text editor which may accidentally corrupt it.

When the license key file expires, to continue using **Dr.Web for IBM Lotus Domino** you have to get a new key file, replace the old one with it, and restart the Lotus Domino server.

Chapter 2. Installation and Removal

The **Dr.Web for IBM Lotus Domino** software is distributed as a single self-extracting archive (**drweb-domino-600-linux-x86.run**).

It is recommended to use only files from official Doctor Web CDs/DVDs or downloaded from the Downloads section of the company's web site.

The archive contains the following packets which are automatically installed after extraction:

Name	Description
drweb-common	Contains: • main configuration file **drweb32.ini** • libraries • documentation • directory structure When this packet is installed, it creates: • **drweb** user • **drweb** group
drweb-bases	Contains: • antivirus scanning engine • virus databases (VDB) Requires drweb-common.
drweb-libvaderetro	Contains the Vade Retro anti-spam library **libvaderetro.so**.
drweb-updater	Contains the updater of the antivirus engine, virus databases and the anti-spam library. Requires drweb-common.

Name	Description
drweb-daemon	Contains the **Dr.Web Daemon** executables and its documentation. Requires drweb-bases.
drweb-scanner	Contains the **Dr.Web Scanner** executables and its documentation. Requires drweb-bases.
drweb-lotus-plugin7	Contains: • binary files • configuration files • script for final adjustments • init-scripts
drweb-lotus-plugin8	Contains: • binary files • configuration files • script for final adjustments • init-scripts
drweb-lotus-plugin-templates-en	Contains English templates for service NSFs. Not compatible with drweb-lotus-plugin-templates-ru.
drweb-lotus-plugin-templates-ru	Contains Russian templates for service NSFs. Not compatible with drweb-lotus-plugin-templates-en.
drweb-libs	Contains libraries, common for all **Dr.Web for IBM Lotus Domino** components.
drweb-epm6.0.0-libs	Contains libraries for graphic installer and uninstaller. Requires drweb-libs packet.
drweb-epm6.0.0-uninst	Contains files of graphic uninstaller. Requires drweb-epm6.0.0-libs packet.
drweb-agent	Contains **Dr.Web Agent** executable files, libraries and documentation. Requires drweb-boost144 and drweb-common packets.
drweb-boost144	Contains libraries, used by **Dr.Web Agent**. Requires drweb-libs.

Name	Description
drweb-monitor	Contains **Dr.Web Monitor** executable files, libraries and documentation. Requires drweb-boost144 and drweb-common packets.

Before installing **Dr.Web for IBM Lotus Domino** carefully analyze the configuration of your Lotus Domino environment and select a server which will serve as the center of its anti-virus and anti-spam protection.

For proper installation and removal of **Dr.Web for IBM Lotus Domino** the user must have "root" privileges or be able to execute actions using the "sudo" command on the computer where the Lotus Domino server is installed.

Dr.Web for IBM Lotus Domino is not compatible with other anti-virus software. Installing two anti-virus programs on one computer may lead to system crash and loss of important data. If you already have an earlier version of **Dr.Web for IBM Lotus Domino** or other anti-virus software installed, it is necessary to uninstall it using the installation file or standard tools of the OS (see Removing Dr.Web for IBM Lotus Domino).

System Requirements

This section provides system requirements for installation and proper operation of **Dr.Web for IBM Lotus Domino** on your computer.

Hardware requirements

Specification	Requirement
CPU	Pentium 133 MHz or higher; has to be compatible with the i80386 command system
RAM	64 MB or more.
Disk space	90 MB or more
Monitor	VGA-compatible monitor with recommended capable to display at least 1280 x 1024 pixels with 256 colors

OS and software requirements

Specification	Requirement
OS	32-bit: • Red Hat Enterprise Linux (RHEL) version 4, 5 and 6 • Novell SuSE Linux Enterprise Server (SLES) version 9, 10 and 11
Lotus software	Lotus Domino 7.x for Linux Lotus Domino 8.x for Linux Lotus Notes 6.5 for Windows or later version
Other	For product work (in particular, for anti-virus demon drwebd) it is necessary to disable Security-Enhanced Linux.

Dr.Web for IBM Lotus Domino does not support 64-bit versions of IBM Lotus Domino.

Doctor Web does not guarantee operation of **Dr.Web for IBM Lotus Domino** on alpha, beta and other non-release versions of the Lotus Domino server.

Installing Dr.Web for IBM Lotus Domino

Before installation it is strongly recommended to:

- install all critical updates released for the OS used on your computer
- check the file system with the system utilities and remove the detected defects

To install Dr.Web for IBM Lotus Domino using the GUI installer:

1. Stop the Lotus Domino server.
2. Remove any previous versions of the plug-in and other anti-viruses for IBM Lotus Domino.
3. Allow execution of **drweb-domino-600-linux-x86.run**. E.g. you can use the following command: `# chmod +x drweb-domino-600-linux-x86.run`
4. Execute the file: `# ./drweb-domino-600-linux-x86.run`
5. The **drweb-lotus-6.0.[release].[path]-[build]_linux** folder will be created with a set of installation files and the GUI installer will start.
6. Select the necessary packet depending on the IBM Lotus Domino version. Click **Next**.
7. In the next window you will be offered to read the License agreement (you can choose the language of License agreement display in the **Languages** list). You should accept it and click **Next** in order to continue installation.
8. The installation of **Dr.Web for IBM Lotus Domino** will start.
9. After successful installation the **Installation complete** message will appear. To run the script to configure the program, select the **Run interactive postinstall script** checkbox and c lick **Next**. As a result, the script will perform the following steps:
    - license key file will be copied to **/opt/drweb** folder;
    - path to key file will be added to configuration files of **Dr.Web Agent** and **drwebd** daemon;

- for **Dr.Web Monitor**, **drwebd** and **drweb-lotusd** daemons automatic start will be set;
- **Dr.Web Monitor**, **drwebd** and **drweb-lotusd** daemons will be started.

10. Click **Close** to exit the installer.

To install Dr.Web for IBM Lotus Domino using the console (without the GUI installer):

1. Stop the Lotus Domino server.
2. Remove any previous versions of the plug-in and other anti-viruses for IBM Lotus Domino.
3. Allow execution of **drweb-domino-600-linux-x86.run**. E.g. you can use the following command: # chmod +x drweb-domino-600-linux-x86.run
4. The **drweblotus-6.0.[release].[path]-[build]_linux** folder containing file set will be created during extraction.
5. Select the necessary installation packet depending on the IBM Lotus Domino version. Click **Next**.
6. In the next window you will be offered to read the License agreement. You should accept it and click **Next** in order to continue installation.
7. The installation of **Dr.Web for IBM Lotus Domino** will start.
8. Further you can adjust main program components. If you agree, the following actions will be performed:
   - license key file will be copied to **/opt/drweb** folder;
   - path to key file will be added to configuration files of **Dr.Web Agent** and **drwebd** daemon;
   - for **Dr.Web Monitor**, drwebd and **drweb-lotusd** daemons automatic start will be set;
   - **Dr.Web Monitor**, **drwebd** and **drweb-lotusd** daemons will be started.
9. After successful installation the **Installation complete** message will appear.

Additional Information about the Installation

The following actions occur during installation of **Dr.Web for IBM Lotus Domino**:

- Originals of the distribution kit configuration files (***.N**) are written to the **/etc/drweb/software/conf** directory.
- Configuration files are installed to the corresponding system directories.
- All other files are installed. If a file with a certain name already exists (e.g. it was left after removal of other packets), it is replaced by a new one and a copy of it is saved as **[file_name].O**.

Installation on Several Servers

When installing **Dr.Web for IBM Lotus Domino** on several servers in one Domino domain, it is necessary to replicate the server's address book (the **names.nsf** database which can be found in the **Data** folder of the server) to all other Lotus Domino servers in the domain after every installation. If you do not replicate the **names.nsf** database, duplicates of the **DrWeb Admin** group will appear in the address book and it will become impossible to send mail notifications to the administrator.

If the situation described above occurs:

1. Move the users from one **DrWeb Admin** group to another by editing the group's document in the **names.nsf** database.
2. Remove the empty duplicate of the **Drweb Admin** group.
3. Replicate the **names.nsf** database to all Lotus Domino servers in the domain (see the IBM Lotus Domino documentation: http://www.ibm.com/developerworks/lotus/documentation/domino/).

Post-installation Setup

Component interaction setup

To enable and set up interaction between components the **drweb-lotus-install.sh** script is used. It uses default settings which may be changed:

- In the **/etc/drweb/drweblotus-setup.conf** file you can specify the path to the Lotus Domino server, user and server launch group name, sockets used by the **drwebd** and **drweblotusd** daemons and some additional parameters.
- If you did not select the **Run interactive postinstall script** checkbox during installation, specify the `ENABLE=1` parameter in the **/etc/drweb/drwebd.enable** and **/etc/drweb/drweb-lotusd.enable** files to enable daemons (**drwebd** и **drweblotusd**).

After you make sure that the settings are correct, run the **/opt/drweb/scripts/lotus/drweb-lotus-install.sh** script which will set up the interaction of the Lotus Domino server with the plug-in. The script performs the following actions:

- Creates necessary NSF databases in the **/local/notesdata/DrWeb** directory**.**
- Creates necessary mnemonic links to binary files of **Dr.Web for IBM Lotus Domino**.
- Adds the necessary parameters to the **notes.ini** file of the Lotus Domino server (see Changes in the Lotus Domino Server Directory).

Signing the service databases

After installation it is necessary to sign the new Domino server databases used by **Dr.Web for IBM Lotus Domino**. If you do not sign the databases then the plug-in will not be able to automatically generate reports and clean the **Quarantine**.

To sign the databases:

1. Make sure that you have administrator rights for the Lotus Domino server.
2. Start the Lotus Domino server.
3. Start the Domino Administrator client.
4. Click the **Open Server** item in the **File** menu and select the server where **Dr.Web for IBM Lotus Domino** is installed.
5. In the **Files** tab select all the **Dr.Web for IBM Lotus Domino** databases from the **DrWeb** subdirectory of the Lotus Domino **Data** folder. The databases are: **DrWebAdmin.nsf**, **DrWebDesign.nsf**, **Quarantine.nsf**, **DrWebReports.nsf**, **DrWebHelp.nsf**, **DrWebLog.nsf, DrWebSpam.nsf**.
6. Right click the databases and select the **Sign...** item for them or click the **Sign...** item in the **Tools** --> **Database** menu in the right part of the Domino Administrator client.
7. Select **Active Server`s ID** in the **Sign Database** window and click **OK**.

Key file access setup

If you did not select the **Run interactive postinstall script** checkbox during installation, it is necessary to specify the path to the key file and enable access to it for all components which require it:

- After receiving the **Dr.Web for IBM Lotus Domino** key file it is necessary to enable reading access for the account from which the Lotus Domino server is started. Then it is necessary to specify a path to the key file as **LicenseFile** parameter value in the **StandaloneMode** section in the **/etc/drweb/agent.conf** configuration file
- If you also received the anti-virus daemon (**drwebd**) key file, it is necessary to enable reading access for the **drweb** user. Then it is necessary to make sure that the path to the key file in the **Key** parameter of the daemon settings file (**/etc/drweb/drweb32.ini**) is specified correctly, e.g. `Key=/opt/drweb/drweb32.key`

Starting the daemons

If you did not select the **Run interactive postinstall script** checkbox during installation (thus, the script of program components adjustment did not run), then it is necessary to start the daemons (**drwebd** и **drweblotusd**).

To start the drwebd anti-virus daemon:

- Execute the following command: `service drwebd start`

The daemon will then start automatically every time the OS launches.

To start the drweblotusd auxiliary daemon:

- Execute the following command: `service drweb-lotusd start`

The daemon will then start automatically every time the OS launches.

Launch and Configure Dr.Web Monitor

If you did not select the **Run interactive postinstall script** checkbox during installation (thus, the script of program components adjustment did not run), then it is necessary to configure **Dr.Web Monitor**.

To configure Dr.Web Monitor:

1. Open the **/etc/drweb/drweb-monitor.enable** file and set the parameter value `ENABLE=1`.
2. Launch **Dr.Web Monitor** by the following command:
   `/etc/init.d/drweb-monitor start`

   Make sure that there were no start up errors.

Removing Dr.Web for IBM Lotus Domino

If you uninstall **Dr.Web for IBM Lotus Domino**, all your groups and profiles, scanning and report settings will be lost; the Quarantine and incidents database (**Quarantine.nsf**) will be deleted.

To remove Dr.Web for IBM Lotus Domino using the GUI installer:

1. Stop the Lotus Domino server.
2. Run the following script: **/opt/drweb/scripts/lotus/drweb-lotus-remove.sh**
3. Open the **drweb-lotus-6.0.[release].[path]-[build]_linux** directory (it is created in the directory where the **Dr.Web for IBM Lotus Domino** self-extracting installation archive was launched).
4. Run the following command: `# ./uninst`
5. Click the **Remove** button.
6. Click close when the removal finishes.

To remove Dr.Web for IBM Lotus Domino via the console (without the GUI installer):

1. Stop the Lotus Domino server.
2. Run the following script: **/opt/drweb/scripts/lotus/drweb-lotus-remove.sh**
3. Run all the removal files (***.remove**) of the installed packets: `# /drweb-lotus-6.0.[release].[path]-[build]_linux/[`*имя_файла*`].remove`

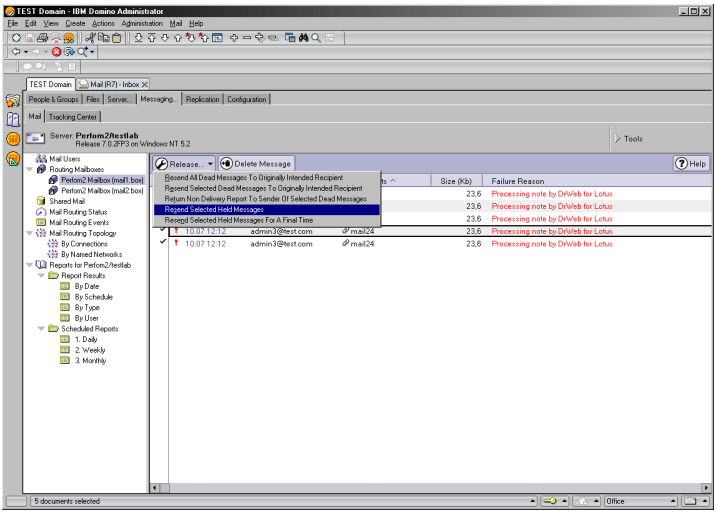
After removing **Dr.Web for IBM Lotus Domino** it is necessary to manually delete the **DrWeb Admin** group.

Post-removal Setup

After removing **Dr.Web for IBM Lotus Domino** some e-mail messages may be left pending on the Lotus Domino server unchecked because all messages acquire the **HOLD** status before they are processed by the plug-in.

To send these e-mail messages to their recipients:

1. Start the Lotus Domino server.
2. Start the Domino Administrator client.
3. Click the **Open Server** item in the **File** menu and select the server where **Dr.Web for IBM Lotus Domino** was installed.
4. Open the **Messaging** tab and check the mailboxes (under **Routing Mailboxes** in the menu on the left) for e-mail messages with the **Processing note by DrWeb for Lotus** comment in the **Failure Reason** column (see illustration below).



5. Select the messages which have been held by **Dr.Web for IBM Lotus Domino** and click the **Release** button above the list.
6. Right-click the selected messages and click **Resend Selected Held Messages**.

Released e-mail messages will be sent to their recipients and will not be checked by **Dr.Web for IBM Lotus Domino** because it has already been uninstalled.

Chapter 3. Getting Started

This chapter contains information on how to review a successful installation and start the Administrator Console.

Post-installation Review

Before starting the Lotus Domino server and changing the default settings of **Dr.Web for IBM Lotus Domino**, it is recommended to make sure that the plug-in is installed correctly and is fully functional. This section contains all the information required to verify a correct installation.

Main Folders and Files which are Created During Installation

Make sure that the following directories have been created during the installation of **Dr.Web for IBM Lotus Domino** and contain all the necessary files in them:

Directory	File name	Description
/opt/drweb	drwebd	Anti-virus daemon
	drweblotusd	Auxiliary daemon (anti-spam, statistics, etc.)
	update.pl	Update script
	drwebd.key	Key file of the anti-virus daemon
	drweb-agent	**Dr.Web Agent** file
	drweb-monitor	**Dr.Web Monitor** file
/opt/drweb/lotus	libdrwebmonitor.so	Library with hook
	drwebmonitor	Binary executive file — mail monitor (server task)
	drwebscanner	Binary executive file — scanner for checking NSF databases according to schedule (server task)
	setup	Binary executive file for creating NSF databases from NTFs. Starts during installation and is deleted after
/opt/drweb/lotus/templates	*.ntf	Database templates for creating NSFs
/local/notesdata/DrWeb	DrWebAdmin.nsf	Administrator console
	DrWebDesign.nsf	Service database
	Quarantine.nsf	Quarantine and incidents database
	DrWebReports.nsf	Reports database
	DrWebHelp.nsf	On-line help database

Directory	File name	Description
	DrWebLog.nsf	Event log database
	DrWebSpam.nsf	SPAM-messages database
/etc/drweb	drweblotusd.conf	Configuration file of the auxiliary daemon (**drweblotusd**)
	agent.conf	Configuration file of **Dr.Web Agent**
	monitor.conf	Configuration file of **Dr.Web Monitor**
/var/drweb/run	drweblotusd.pid	File with the current process identifier of the auxiliary daemon (**drweblotusd**)
	drweb-agent.pid	File with the current process identifier of the **drweb-agent** daemon
	drweb-monitor.pid	File with the current process identifier for **Dr.Web Monitor**
/var/drweb/lib	libvaderetro.so	Anti-spam library

Changes in the Lotus Domino Server Directory

During installation of **Dr.Web for IBM Lotus Domino** the **DrWeb Admin** group is automatically created in the Lotus Domino server address directory (the **names.nsf** database). The group is specified in the *Access Control Lists* (ACL) of all the databases of the plug-in. The administrator of the server, specified in the **notes.ini** file of the server (the **Admin** parameter) is added to this group by default. The administrator can also add other Lotus Domino users who will perform administrator duties to the **DrWeb Admin** group. This group is used to send notifications on the operation of **Dr.Web for IBM Lotus Domino**. Deleting this group will lead to problems with notifications and access to databases of the plug-in.

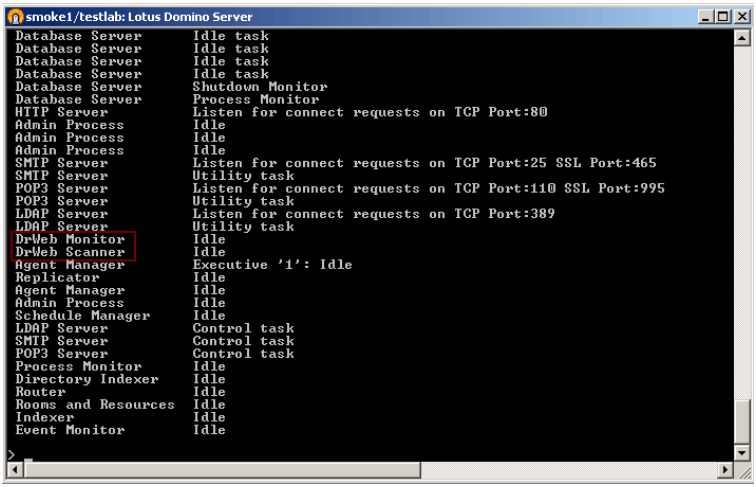
Also, the following changes are made in the **notes.ini** file of the server:

- The **nmonitor.dll** value is added to the **EXTMGR_ADDINS** parameter.
- The **drwebmonitor** and **drwebscanner** tasks are added to the **ServerTasks** parameter.
- The **DrWebBuild** parameter (it's value represents the build number) is added.
- The **DrWebSocket** and **DrWebVRSocket** parameters are added which are used to specify the UNIX-socket, TCP-socket or PID-file for interaction with the **drwebd** anti-virus daemon (by default **pid:/var/drweb/run/drwebd.pid**) and the **drweblotusd** auxiliary daemon (by default **/var/drweb/lotus/.vrsocket**).

If you do not wish the plug-in's virus detection features to automatically load when you start the Lotus Domino server, you should delete the **drwebmonitor** value from the **EXTMGR_ADDINS** parameter and the **drwebmonitor** and **drwebscanner** values from the **ServerTasks** parameter.

Launching the Lotus Domino Server

If **Dr.Web for IBM Lotus Domino** was installed successfully, you can start the Lotus Domino server. To make sure that the **Monitor** and **Scanner** tasks of the plug-in have been launched use the `sh task` command. Below is the illustration of the Lotus Domino Server command window with the correct result of the `sh task` command.



Virus Detection Test

To check the functionality of the plug-in's virus detection capabilities and its default configuration, it is recommended to use the EICAR (European Institute for Computer Antivirus Research) test file. The test file consists of a text string 68 or 70 bytes long, it is not a virus, it cannot replicate and does not contain any payload, however, it is recognized by anti-virus software as a virus. You can download the test file from the EICAR website (http://www.eicar.org) or create it yourself.

To create the EICAR test file:

- Create a text file with the following string:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-
ANTIVIRUS-TEST-FILE!$H+H*
```

Save the file with a **.com** extension (you can use any name, e.g. **eicar.com**), attach it to an e-mail message and send it to any test e-mail address. The received message should contain an attached text file with the **_infected.txt** suffix and the following contents:

```
Dr.Web for IBM Lotus Domino has detected that
memo is infected with a virus.

Date: Mon Mar 31 18:37:47 2008

Sent from: Admin/smoke
Recipients: mail1/smoke
Subject: test message
Viruses: eicar.com ( EICAR Test File (NOT a
Virus!) ) quarantined.
```

Do not use real viruses to check the functionality of anti-virus software!

Components of the Program

Dr.Web for IBM Lotus Domino is a complex anti-virus package which consists of several complementary components that interact with each other to ensure the highest level of anti-virus protection. The operation of these components can be configured via the **Dr.Web Administrator Console** (see Starting the Administrator Console).

Below is a list of these components with their short descriptions:

- **Anti-virus daemon** (**drwebd**) is used to perform anti-virus scanning.
- The **Monitor** (binary executive file **drwebmonitor**) scans mail. box of the Lotus Domino server, i.e. all incoming and outgoing messages in real time mode as they are processed by Lotus Domino. As soon as scanning of a message is complete and it is considered safe, the message is immediately sent to the receiver. If a message contains infected or suspicious objects, then a corresponding prespecified action is applied to it.
- The **Scanner** is used to periodically check documents in the selected NSF databases. It is launched according to schedule or manually and, like the **Monitor**, applies prespecified actions to infected and suspicious objects.
- **Auxiliary daemon** (**drweblotusd**) is used to check all messages for spam and update the anti-spam library (**libvaderetro.so**). It uses special algorithms based on the detection of spam features in e-mail messages to determine whether the message is spam or not. If the component determines that a message is spam then a predefined prefix is added to the message header (by default, the prefix is set to **[SPAM]**).

- The **Quarantine** is used for isolation of infected and suspicious objects. Access to objects in the **Quarantine** is performed via the **Dr.Web Administrator Console** database **(DrWebAdmin.nsf**).
- The **Updater** (**update.pl**) is a Perl script included into the **Dr.Web for IBM Lotus Domino** anti-virus package. It is designed to automatically update the virus databases. The **Updater** downloads copies of the virus databases via the Internet, from a local network folder or server.
- The **Statistics** component (a part of **quarantine.nsf**) saves information on the types of processed messages and actions performed with these messages. You can view this information in order to keep track of the **Dr.Web for IBM Lotus Domino** activity.
- The **Reports** component (**DrWebReports.nsf**) is used to regularly send reports on the operation of **Dr.Web for IBM Lotus Domino** to the specified addresses according to a certain schedule.
- The **Event Log** component allows administrators of the Lotus Domino servers to effectively monitor the events which occur during operation of **Dr.Web for IBM Lotus Domino** (e.g. update of the virus database, detection of a virus, adjustments of settings, etc.). The **Event Log** database (**DrWebLog.nsf**) can contain information from one or several Lotus Domino servers under protection of the anti-virus plug-in. Documents with event information are sent to the **Event Log** via internal mail system of the Lotus Domino server.

Operation of the **Monitor** and **Anti-spam** components can be configured for different profiles to suit the needs of various clients and groups. Operation of other components is configured for the whole plug-in.

Starting the Administrator Console

Once you have made sure that **Dr.Web for IBM Lotus Domino** was installed correctly and checked its functionality with default settings, you can pass on to performing administrative tasks. The operation of **Dr.Web for IBM Lotus Domino** is configured by means of the **Dr.Web Administrator Console**. The console is represented by a GUI which can be launched in Lotus Notes environment or in any supported web browser via the **DrWebAdmin.nsf** database.

For correct displaying of the GUI it is recommended to set the resolution of your monitor to 1280 by 1024 pixels or higher.

Operation of the web console requires the HTTP server task to be launched on the Lotus Domino server.

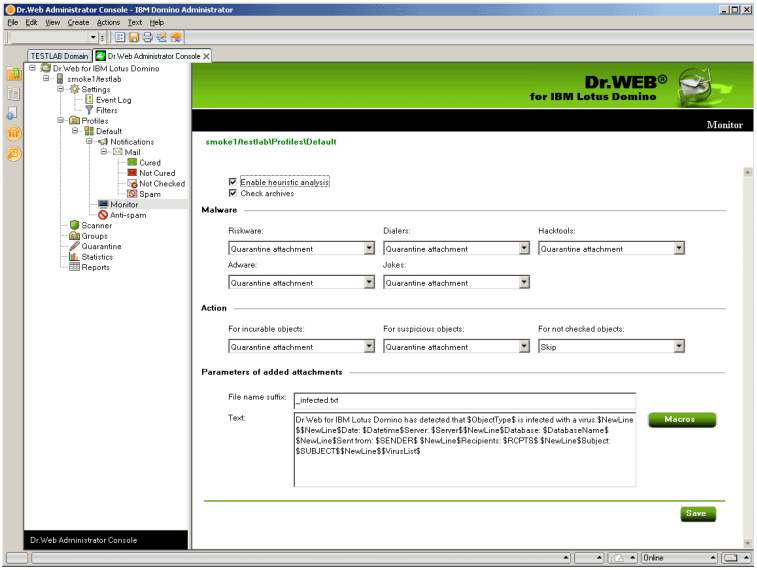
To launch the Dr.Web Administrator Console in Lotus Notes:

1. Start the Lotus Domino server.
2. Start the Lotus Notes client software.
3. Open the **File** menu, select the **Database** item and click **Open**. This will bring up the **Open Database** window (alternatively, you can press CTRL+O on the keyboard to do this).
4. Select a Lotus Domino server with the installed plug-in from the drop-down list at the top of the **Open Database** window.
5. Select the **Dr.Web Administrator Console** database (**DrWebAdmin.nsf**) in the **DrWeb** subfolder and click **Open**.

To launch the Dr.Web Administrator Console in a web browser:

1. Start the Lotus Domino server.
2. Start a web browser.
3. Go to the following URL: http://domino.server/drweb/drwebAdmin.nsf
4. Enter the name and Internet password of the administrator account specified in **DrWeb Admin** group.

The **Dr.Web Administrator Console** consists of two parts (see illustration below). On the left is the hierarchical menu used for navigation between different sections of the program settings. In the right part of the window is the frame with the working area where the settings of the currently selected section are displayed and can be adjusted. At the top of the frame with the working area is the name and logo of **Dr.Web for IBM Lotus Domino** and the name of the current settings section.



Getting Help

An integrated help system is implemented in **Dr.Web for IBM Lotus Domino**. It is a separate NSF database (**DrWebHelp.nsf**) which is installed to the `\DATA\DRWEB` folder. Open this database in Lotus Notes to access the main help system.

To access a section of the help system depending on the context (i.e. the currently selected section in the **Administrator Console**), press the F1 key on the keyboard.

Also, the **About Dr.Web for IBM Lotus Domino** section with information about the version of **Dr.Web for IBM Lotus Domino** is available via the top item of the hierarchical menu in the **Administrator Console** (see illustration in Starting the Administrator Console). In this section you can view information about your key file, versions of all program components and last update of the virus database. This information is required for analysing bugs and errors when contacting technical support.

Chapter 4. Administration

This chapter contains information on understanding the structure of **Dr.Web for IBM Lotus Domino** and performing all the administrative tasks required to ensure the ultimate protection for your Lotus Domino environment.

Groups and Profiles

To simplify management of your Lotus Domino environment **Dr.Web for IBM Lotus Domino** provides the ability to form groups of clients and assign profiles to them. A profile is a set of adjustable message processing settings which determine how the protection of your Lotus Domino environment is carried out. The settings of a profile can be found in the **Profiles** section of the hierarchical menu and are divided into the following subsections:

- Notifications - this section allows you to set up notifications which can be used to keep the administrator and other users informed about various events (e.g. detection of infected or suspicious messages, attempts to cure them, filtering of messages, etc.);
- Monitor - this section allows you to control the way your main virus-detection component performs;
- Anti-spam - this section allows you to adjust the operation of the **Anti-spam** component (settings in this section can be enabled only with the "Anti-virus + Anti-spam" version of **Dr.Web for IBM Lotus Domino**, i.e. if you have an appropriate license key file (see License Key File)).

More detailed information on creating and managing profiles can be found in Creating and Managing Profiles.

Any profile can be assigned to a certain group of clients. These groups are formed in the **Groups** section of the hierarchical menu (see Managing Groups of Clients).

Creating and Managing Profiles

Profiles determine different sets of parameters for anti-virus scanning and anti-spam filtering, actions applied to detected objects and distribution of notifications.

During the installation of **Dr.Web for IBM Lotus Domino** the **Default** profile is created. This profile will remain active for all Lotus clients as long as you do not specify a different one.

It is impossible to delete or rename the **Default** profile and its parameters are set automatically for all newly created profiles.

To create a new profile:

1. In the hierarchical menu click the **Profiles** item and select **Add New** under the list of profiles to the right.
2. Choose a name for the profile and click **OK**. A new profile will be created and a new item will appear under **Profiles** in the hierarchical menu.

   ### To change the name of a profile:

   - Select the profile in the hierarchical menu, enter the desired name in the **Name** field and click the **Save** button.

The following symbols are not allowed in the name of the profile: **! / \ | ; : " * ,**

3. Once created, a new profile has settings similar to the **Default** profile.

   ### To change parameters of the new profile:

   - Click the name of the profile in the hierarchical menu and choose the settings you wish to adjust (Notifications, Monitor or Anti-spam).

Setting Up Notifications

Notifications are used to keep the administrator and other users informed about various events (detection of infected or suspicious documents, attempts to cure them, filtering of spam messages, etc.).

To open the Notifications frame with the notifications settings for a profile:

- Select the profile in the hierarchical menu and click the **Notifications** item.

By default, all notifications are disabled.

To set up mail notifications:

1. Click the **Mail** item under **Notifications** and select what type of events you wish to set up notifications for:
   - **Cured** - when an infected object is detected and cured;
   - **Not Cured** - when the detected object cannot be cured;
   - **Not checked** - when the message could not be checked;
   - **Spam** - when the received object is considered spam.
2. For each event type you can set up separate notifications for the administrator, sender and receiver; for this switch between the corresponding tabs at the top of the frame (see illustration below).

3. To enable the sending of mail notifications for the necessary event type:
   - Select the **Send Mail notifications** check box.
4. Adjust the template of mail notifications in the **Header** and **Body** fields below. You can add macros to the notification body by clicking the **Macros** button and selecting them from the list.
5. The recipients of notifications can be edited only in the

Administrator tab. You can add users to this entry field by clicking the **Add** button and selecting them in the **Select Addresses** window.

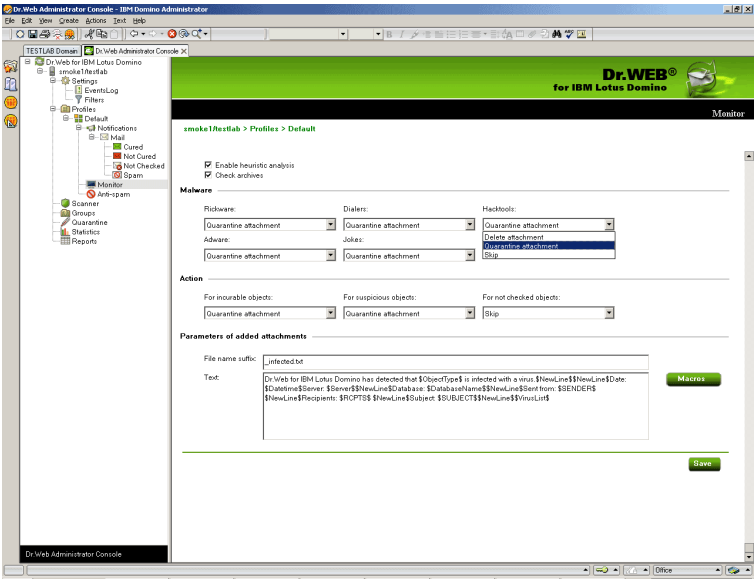
6. Edit the **Sender** field if necessary.
7. When you are done click **Save**.

Adjusting the Monitor

The **Monitor** scans all incoming and outgoing messages in real time mode as they are processed by Lotus Domino. Its operation can be adjusted for different profiles to suit the needs of various groups of clients.

To adjust the parameters of the Monitor operation:

- Select the necessary profile in the hierarchical menu and click the **Monitor** item.



The illustration above shows the **Monitor** frame.

By default, the heuristic analyzer and scanning of archives in attachments are enabled. This gives a high level of protection at the expense of the server's computational resources. To disable these features clear the **Enable heuristic analysis** and **Check archives** check boxes at the top of the **Monitor** frame.

It is not recommended to disable the heuristic analyzer as it decreases the protection level of the server greatly. In the Linux version of **Dr.Web for IBM Lotus Domino** scanning of archives in attachments is always performed, even if the corresponding check box is not selected. This is a temporary feature.

In the **Malware** group box you can choose actions for various types of potentially malicious programs and in the **Action** group box you can choose actions for incurable, suspicious objects and those which could not be checked. Use the corresponding drop-down lists to choose from the following actions:

- **Delete attachment** - means that the message body will be passed through and the attachment will be replaced by a text file with the time of detection, information on the detected virus and performed action (available only for suspicious, incurable objects and malware).
- **Quarantine attachment** - means that the message body will be passed through and the attachment will be sent to the **Quarantine** database (see Managing the Quarantine). A text file with the time of detection, information on the detected virus and performed action is attached to the e-mail.
- **Skip** - means that the message will be passed on to the receiver without any actions applied to it or its attachment (available for objects which could not be checked and malware).

In the **Parameters of added attachments** group box you can change the suffix for the name of the text file attached to an infected e-mail message when an action is carried out with it (i.e. the new file name will consist of the original name with the suffix added at the end). In the **Text** field below you can edit the text of the attached text file template if necessary.

To add a new macro to the template:

- click the **Macro** button, select the desired macro in the opened window and click **Select**.

When you finish adjusting the **Monitor** component click **Save**.

Setting Up Anti-spam Filtering

Spam detection is performed by the **Anti-spam** component which analyses the contents of e-mail messages and defines whether it is spam or not according to the spam-rate value summed up from various criteria (the spam message is also related to a certain category according to how likely it is that the message contains spam: *Certainly spam*, *Probably spam* or *Unlikely spam*). For each category you can specify a certain action (see below for description of **Anti-spam** settings).

The **Anti-spam** component is available only with the "Anti-virus + Anti-spam" version of **Dr.Web for IBM Lotus Domino**. If your key file supports the **Anti-spam** component then spam detection should be enabled by default.

If all the settings in the **Anti-spam** frame are disabled then it is likely that your license key file does not support the **Anti-spam** component (see License Key File). To check this, you can open the key file (**/local/notesdata/drweb32.key**) with a text editor and look for the following string: `LotusSpamFilter=No`.

To set up the Anti-spam for a profile:

1. Make sure that your version of the program includes the **Anti-spam** component.
2. Choose the necessary profile in the hierarchical menu and click the **Anti-spam** item.
3. By default, the **Anti-spam** component is enabled. If it is not, you can enable the component by selecting the **Enable** check box.
4. If you want a prefix to be added to the subject fields of spam messages, select the **Change subject** check box. You can edit the prefix itself in the **Subject prefix** entry field (by default, it is set to **[SPAM]**).

5. Besides adding a prefix to the subject of spam messages, you can select actions for various categories:
   - **Move to database for spam** - means that the spam message will be moved to the database specified in the **Database for spam** text box (if the specified database is not found, the spam message will be passed on to the receiver). You can also specify a certain folder inside the database in the **Folder** text box and the spam message will be moved to this folder (if this folder is not found in the database, the spam message will still be moved to the database but not inside a folder).
   - **Reject message** - means that the spam message will be received by the server and deleted without passing it on to the receiver. However, a document for this incident will be created in the **Quarantine.nsf** database.
   - **None** - means that no action will be applied to the message and it will be passed on to the receiver (the subject will still be changed if the **Change subject** check box is selected for this category).

To keep spam-messages, use any of the Notes databases, based on the standard postal template, for example, Mail7.ntf. Besides, DrWebSpam.nsf database is supplied with **Dr.Web** plug-in. DrWebSpam.nsf is installed in the Drweb subfolder of the Lotus Domino server data folder. This database is based on the template, similar to quarantine and incidents database, and it provides some extra functions, which can be useful for spam processing: several types of filters, blocking from removal, automatic removal of old messages, delivery of the messages, that were wrongly classified as spam, to user. It also allows to add senders to white or black list.

6. When you finish adjusting the **Anti-spam** component, click **Save**.

If the spam filter regards certain messages as spam by mistake, you are advised to forward such messages to special e-mail addresses for analysis. Messages which are wrongly regarded as spam should be forwarded to vrnonspam@drweb.com, and unblocked spam messages should be forwarded to vrspam@drweb.com. Forward messages as attachments; do not include them to the message body.

Managing Groups of Clients

By default, **Dr.Web for IBM Lotus Domino** applies the parameters of the **Default** profile to all users. If you wish to apply parameters of a different profile for certain users (see Creating and Managing Profiles), then you must include such users into a group and assign the profile to it. Thus, to simplify the management of Lotus clients they can be divided into groups each with its own set of protection parameters.

To create a new group and assign a profile to it:

1. Select the **Groups** item in the hierarchical menu and click the **Add new** button under the list of groups.
2. Choose a name for the group and click **OK**. A new group will be created and a new item will appear under **Groups** in the hierarchical menu.

   ### To change the name of a group:

   - Select the group in the hierarchical menu and enter the desired name in the **Name** field.

The following symbols are not allowed in the name of the group: **!** **/ \ | ; : " * ,**

3. Specify the names of desired Lotus groups in the **Members** entry field via the **Add** button.
4. In the **Profile** field select the profile you want to use for this group.
5. When you finish adjusting the group`s settings click **Save**.

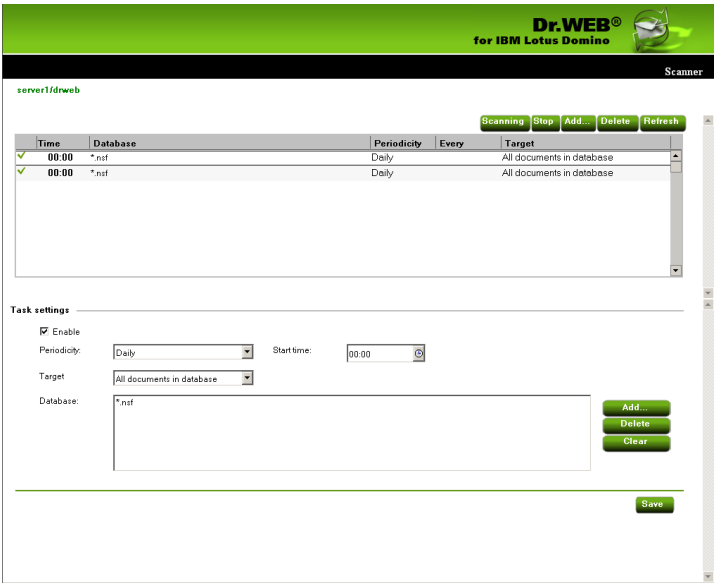
Scanning Lotus Notes Databases

Dr.Web for IBM Lotus Domino can check documents in certain NSF databases according to schedule or by starting the scanning process manually. This is performed by the **Scanner**.

The schedule is formed by tasks which determine the periodicity, time and day of scanning as well as the databases which should be checked.

To set up a task for scanning:

1. Select the **Scanner** item in the hierarchical menu and click the **Add New** button under the list of tasks in the top part of the **Scanner** frame (see illustration below).



2. A new task with default values will appear in the list.
3. Select the newly created task and specify the time parameters for it in the bottom part of the **Scanner** frame (**Task settings** group box). Then add the databases, documents in which you

wish to be checked, to the **Database** list by clicking the **Add** button and selecting the databases from the **Show databases** window.

You can choose either separate databases or specify ***.nsf** to select all databases in a certain folder.

4. In the **Target** drop-down list you can select to scan all the documents in the specified databases or only new and modified ones (the latter means incremental scanning which can help you save time and server computational resources).

If you select to scan only new and modified documents and the scanner does not detect malware in an infected document due to outdated virus database then the document will never be rescanned during incremental scanning unless it is modified. It is therefore recommended to periodically update the virus database and perform a full manual scan at least once a week.

5. When you set up all the parameters for the task select the **Enable** check-box to activate it.

Every minute the **Scanner** verifies the parameters of all active tasks in the list. If these parameters comply with the current date and time then the **Scanner** begins to check documents in the specified databases.

To start the scanning process manually:

- Select the necessary task from and click **Scanning**. This will trigger the selected task and the **Scanner** will begin to check documents in the specified databases within 1 minute.

To stop the scanning process:

- Select the necessary task and click the **Stop** button (it takes up to 1 minute to stop the scanning process).

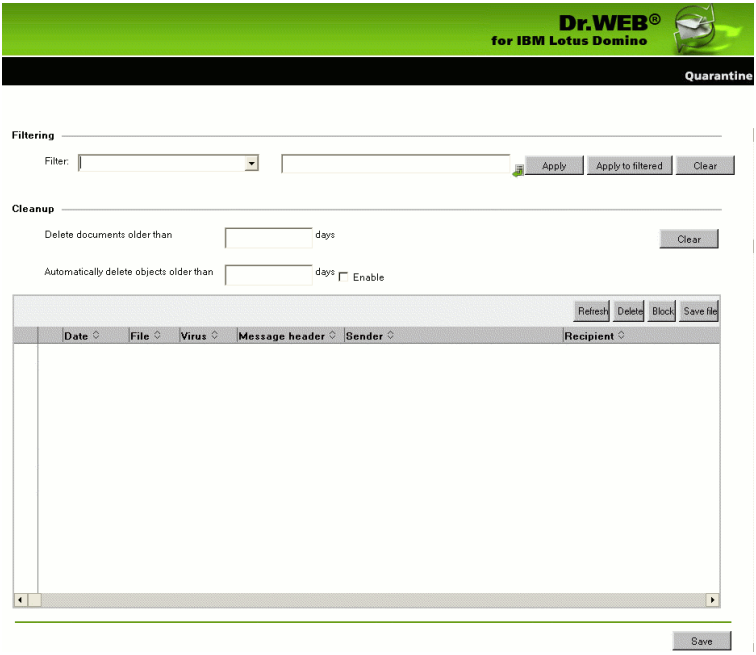
You can start and stop as many scanning tasks as you wish irrespective to each other.

When you finish setting up the scanning tasks, click **Save**.

Managing the Quarantine

The **Quarantine** is a service database (**quarantine.nsf**) which is used to isolate infected and suspicious objects. The **Monitor** and the **Scanner** place such objects in the **quarantine.nsf** database in the form of documents when the **Move to quarantine** action is applied to them.

The **Quarantine** frame (see illustration below) consists of a list of objects which reside in the **Quarantine** and a number of settings for adjusting the list and managing these objects. To sort the list according to certain criteria click the headings of the corresponding columns.



In the **Filtering** group box you can choose to filter the list according to certain criteria.

To filter the list:

1. Select the type of criteria in the **Filter** drop-down list and enter the desired value in the field to the right.
2. Click **Apply** or **Apply to filtered**.

Filters are not applied to the objects themselves but to entries in the list. You can always view the list without filters by clicking the **Clear** button.

In the **Cleanup** group box you can manually delete objects which have been in the **Quarantine** for more than a certain number of days.

To clean up the list:

- Specify the number of days in the corresponding field and click **Clear**.

To delete all documents from the quarantine database you can specify **0** days in the **Cleanup** group box. In this case, when you click **Clear**, the program will ask you whether you are sure that you want to delete all data from the **Quarantine** or not.

You can also specify a certain number of days in the **Automatically delete objects older then** field and select the **Enable** check box next to it to set up automatic cleanup. Automatic cleanup of documents in the **Quarantine** is performed by the **Automatically delete objects** agent in the **quarantine.nsf** database. By default, this agent launches every day at 01:30 AM. You can adjust its settings using standard tools of Lotus Domino (see the IBM Lotus Domino documentation: http://www.ibm.com/developerworks/lotus/documentation/domino/).

To delete a document from the Quarantine:

- Select it in the list and click the **Delete** button.

To save the object, which was moved to the Quarantine, on the hard drive:

1. Select the object.
2. Click the **Save file** button to open a window with the file system tree.
3. Choose the folder you wish to save the object to and click **OK**.

To make a document impossible to delete neither automatically nor manually:

- Select it in the list and click **Block**. Clicking this button again will unblock the document.

The list is automatically refreshed every 12 hours. However, you can refresh it manually at any time by clicking the **Refresh** button.

This process takes some time (up to a few minutes) depending on the amount of objects in the **Quarantine**.

Click the **Save** button at the bottom to save the changes made in the **Quarantine** frame.

Reviewing the Statistics

The **Statistics** component collects information about all the events concerning the **Dr.Web for IBM Lotus Domino** basic functions (detection of infected objects, application of actions to them, filtering of spam, etc.). To view this information select the **Statistics** item in the hierarchical menu. The section is divided into two tabs:

- **Statistics** - contains a brief summary for checked objects, infected objects, cured objects, etc. (statistical information is updated every time an event occurs but no more than once a minute).
- **Incidents** - contains a list of documents with information about the events which occurred during operation of **Dr.Web for IBM Lotus Domino** (virus or spam detection, etc.). Reports are generated according to these documents (see Managing Distribution of Reports).

Settings in the **Incidents** tab are similar to those in the **Quarantine** frame (see Managing the Quarantine). You can sort the list of incidents according to certain criteria by clicking the buttons which denote these criteria at the top of each column. You can also filter the entries in the list to view documents only with a certain date, virus type, etc.

To filter the list:

1. Select the type of criteria in the **Filter** drop-down list and enter the desired value in the field to the right.
2. Click **Apply** or **Apply to filtered**.

To cancel all filters:

- Click the **Clear** button.

If you wish to delete documents which have been in the **Incidents** list for more than a certain number of days, specify this in the **Cleanup** section and click **Clear**.

You can also specify a certain number of days in the **Automatically delete objects older then** field and select the **Enable** check box

next to it to set up automatic cleanup. Automatic cleanup of documents in the **Incidents** list is performed by the **Automatically delete objects** agent in the **quarantine.nsf** database. By default, this agent launches every day at 01:30 AM. You can adjust its settings using standard tools of Lotus Domino (see the IBM Lotus Domino documentation: http://www.ibm.com/developerworks/lotus/documentation/domino/).

To delete a document from the list of incidents:

- Select it in the list and click the **Delete** button.

To make a document impossible to delete neither automatically nor manually:

- Select it in the list and click **Block**. Clicking this button again will unblock the document.

To refresh the Incidents list:

- Click the **Refresh** button above the list.

This process takes some time (up to a few minutes) depending on the amount of objects in the list of incidents.

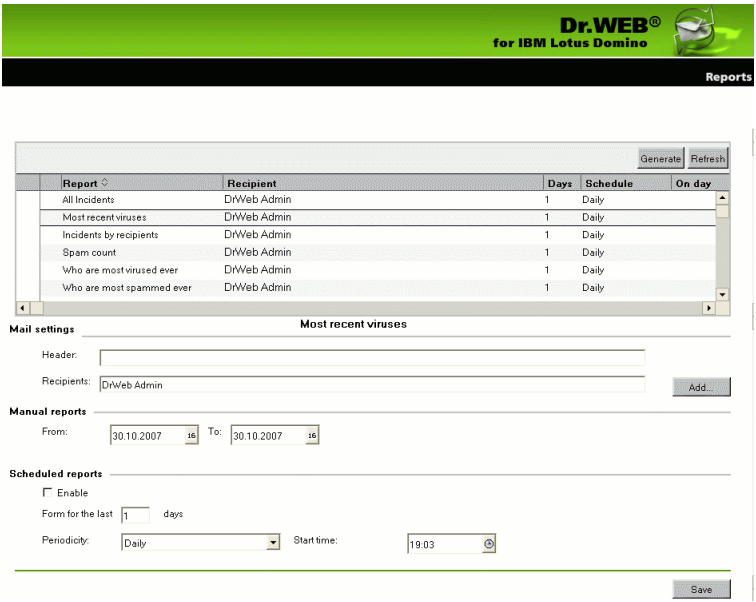
Click the **Save** button at the bottom to save the changes made in the **Incidents** frame.

Managing Distribution of Reports

Dr.Web for IBM Lotus Domino can generate and distribute reports on the operation of the plug-in. These reports are sent as e-mail attachments (HTML files) to addresses which can be specified by the administrator. The reports are based on the list of documents in the **Incidents** tab of the **Statistics** frame.

At the top of the **Reports** frame (see illustration below) is a list of report types which you can set up. There are six types of reports:

- All incidents
- Incidents by recipients
- Most recent viruses
- Spam count
- Who are most virused ever
- Who are most spammed ever



For each type of reports you can specify the subject header and recipients of the e-mail messages with the report type in the **Header** and **Recipients** entry fields under the list of report types (**Mail settings** group box).

To add one or several Lotus Domino clients or a client group to the Recipients field:

- Click the **Add** button next to the entry field and select them in the opened dialog box.

In the **Manual reports** group box you can adjust the dates of incidents for which you wish to manually generate the selected type of reports.

To generate reports manually:

1. Select the necessary report type.
2. Specify the dates in the **From** and **To** entry fields.
3. Click the **Generate** button above the list of report types.

In the **Scheduled reports** group box you can adjust the schedule for automatic distribution of the selected report type.

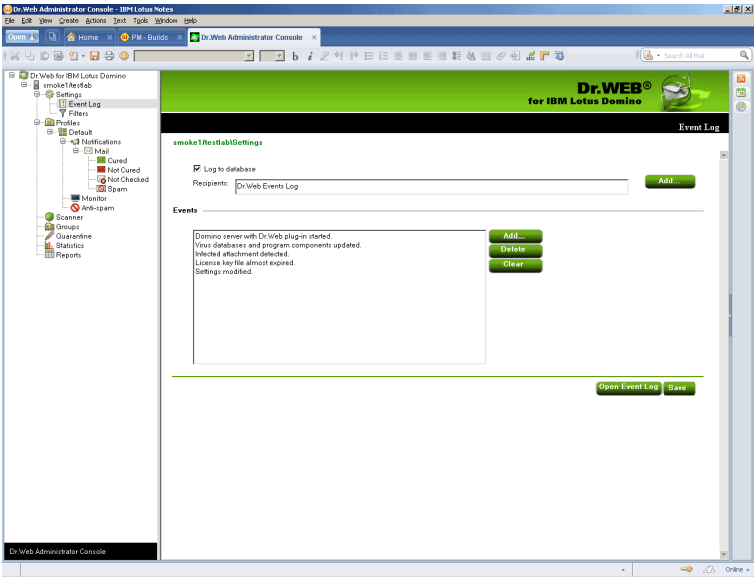
To enable scheduled distribution:

1. Select the **Enable** check box.
2. Specify the number of days (preceding the current day) for which you wish to generate reports (i.e. if you specify "**1**" then only yesterday`s incidents will be included into the report; "**2**" - incidents which occurred in the last two days; etc.).
3. Specify the periodicity, date and time for report distribution
4. Click **Save**.

You cannot set up scheduled reports for the current day. To send a report which would include today's incidents, you have to generate it by specifying a range with the current date in the **Manual reports** group box.

Managing the Event Log

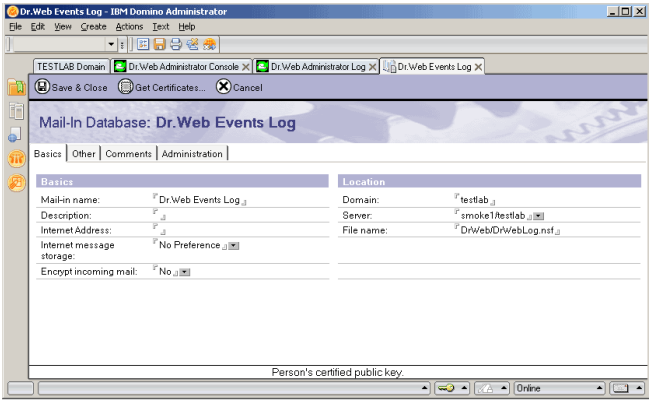
Logging can be useful for network administrators to keep tack of various events during operation of **Dr.Web for IBM Lotus Domino** (especially if there is more than one Lotus Domino server in the network). Logging is adjusted in the **Event Log** subsection of the **Settings** section. The administrator can specify which types of events are logged and where the log database (**DrWebLog.nsf**) is stored.



To start and adjust logging:

1. Click the **Settings** item in the hierarchical menu and then the **Event Log** subitem.
2. Select the **Log to database** check box to enable logging.
3. You can specify a mail address for NSF databases which should be used to save the log by adding them to the **Recipients** field via the **Add** button. Before adding a database to this field, it is necessary to specify a mail address for it:
    1) Start the Domino Administrator client.

2) Select the server and open the **People and Groups** tab.
3) Select the **Mail-In databases and resources** item.
4) Click **Add Mail-In Database**.
5) Choose a name for the database, specify your mail domain name and the server with the Event Log database.
6) Specify `DrWeb/DrWebLog.nsf` in the **File Name** field.



7) Save the new document and replicate the **names.nsf** database to other Lotus Domino servers (if there is more than one).

4. In the **Events** group box you can make up a list of events which you wish to be logged. Use the **Add** and **Delete** buttons to edit the list and the **Clear** button to remove all event types from it.

Click **Save** to apply changes.

Managing Filters for Databases and E-mail Addresses

Filters are used to manage general restrictions for the operation of **Dr. Web for IBM Lotus Domino**. They are adjusted in the **Filters** subsection (the **Settings** section) which is divided into two tabs:

- The Database tab allows you to specify a list of NSF databases either included or excluded from scanning by the **Monitor**.
- The Anti-spam tab allows you to specify black and white lists of e-mail addresses.

The lists can be specified manually (see corresponding tabs in the **Filters** section) or imported from a text file. For lists of included/ excluded databases, the file should contain paths with filenames or masks (in the DATA directory), each starting on a new line, e.g.:

```
mail/gendir.nsf
trustbase/*.nsf
```

For black/white anti-spam lists, the file should contain e-mail addresses or masks, each starting on a new line, e.g.:

```
spamer1@spam.ru
*@spamers.ru
spamer2@spam.ch
```

To import data from a text file into the list:

1. Select the **Settings** item in the hierarchical menu and open the **Filters** section.
2. Click the **Import** button in the lower part of the section to bring up the **Import** dialog window.
3. Select one of the four list types where you wish to import the necessary data.
4. Specify the path and file name.

5. Click the **Import** button.

In the **Results** tab you can view information and statistics on the last imported file.

Filtering Databases

By default, the **Monitor** component of **Dr.Web for IBM Lotus Domino** performs on-access scanning of all NSF databases except some service databases of the Lotus Domino server. Using the **Include** or **Exclude** list in the **Database** tab of the **Filters** section you can create your own restrictions for the operation of the **Monitor**.

Include and **Exclude** lists affect only the operation of the **Monitor** and are not applied to manual or scheduled scanning of NSF databases (see Scanning Lotus Notes Databases).

To set up restrictions for the operation of the Monitor:

- Select the **Enable** check box at the top of the **Filters** frame and add the necessary databases or path templates to one of the lists:
  - **Include** - databases which you wish to be processed (databases not specified in the **Include** list WILL NOT be processed by the **Monitor**);
  - **Exclude** - databases which you do not wish to be processed (databases not specified in the **Exclude** list WILL be processed by the **Monitor**).

To add databases to a list:

1. Click the **Add** button.
2. Select the necessary databases in the opened dialog box and click **OK**.

You can add path templates, i.e. paths to folders containing NSF databases ending with ***.nsf**. E.g. if you specify **mail*.nsf**, all the NSF databases in the **mail** folder of the server's data directory will be added to the list (databases in subfolders will not be added).

To delete a database from the list:

- Select it and click **Delete**.

To clear the list:

- Click the **Clear** button.

When you finish compiling the necessary list of databases, click the **Save** button. Changes will take effect within 1 minute after you save them.

Compiling Black and White Lists of E-mail Addresses

Click the **Anti-spam** tab at the top of the **Filters** frame if you wish to compile black and white lists which determine the behavior of the anti-spam component with distrusted and trusted e-mail addresses respectively.

To add an address to a list:

1. Select the **Enable** check box.
2. Enter an address or domain name in the field below a corresponding list.
3. Click **Add**.

Add e-mail addresses which you trust to the white list (messages from these addresses will not be checked for spam) and addresses which you do not trust to the black list (all messages from it will be considered *Certainly spam* and actions specified in the **Anti-spam** settings for this category will be applied to them).

You can add e-mail addresses and domain names to the black and white lists using templates, i.e. the * symbol. Templates let you specify ranges of addresses or domains (e.g. ***@mail.com** means any address from the **mail.com** domain).

To delete an address from a list:

- Select it and click **Delete**.

To clear a list:

- Click the **Clear** button.

Click **Save** when you finish editing the lists. Changes will take effect within 1 minute after you save them.

Updating the Virus Databases

It is recommended to use the **Updater** script (**update.pl**) to update virus databases and the anti-spam library. The **Updater** is a part of **Dr.Web for IBM Lotus Domino** and can be installed via the **drweb-updater** packet of the installation archive. The actual script is written in Perl and can be found in the directory with the plug-in's executive files (by default: **/opt/drweb/update.pl**).

The **Updater** settings are specified in the **[Updater]** section of the main configuration file (by default: **/etc/drweb/drweb32.ini**). To use a different configuration file, it is necessary to specify the full path to it via a command line parameter when launching the script.

When installing the **drweb-updater** packet, a task for periodic launch of the **update.pl** script (every half an hour) is created via a standard scheduler (**cron**). This is done by creating the **drweb-update** file in the **/etc/cron.d** directory. The file contains the following code:

```
*/30 * * * * drweb /opt/drweb/update.pl
```

When the anti-spam library (**libvaderetro.so**) is updated:

1. The **Updater** script sends a SIGHUP signal to **drweblotusd** daemon using its PID from **drweblotusd.pid** (path to this file is specified in the **Lotusdpidfile** parameter of **drweb32.ini**).
2. The **drweblotusd** daemon copies the new anti-spam library to **/var/drweb/lotus/libvaderetro.so.cache** and loads it into RAM. The old version is deleted.

Configuration Export/Import

Dr.Web for IBM Lotus Domino lets you save the current configuration to a file in order to use the settings on other servers where the plug-in is installed.

To export the current settings:

1. Open the **Dr.Web Administrator Console**.
2. Select the item with the name of the server in the hierarchical menu.
3. Open the **Actions** menu in the top part of the Lotus Notes client window and select the **Export** item.
4. In the opened dialog window select the **Enable** check box and specify the path and file name of the output file in the **Export configuration** group box.
5. Click **Export**.

To import the current settings:

1. Open the **Dr.Web Administrator Console**.
2. Select the item with the name of the server in the hierarchical menu.
3. Open the **Actions** menu in the top part of the Lotus Notes client window and select the **Import** item.
4. Select the server to which you wish to import the configuration and select the **DrWeb/DrWebAdmin.nsf** on this server.
5. In the **Import configuration** group box select the settings you wish to import and the XML file with the configuration.
6. Click **Import**.

When importing configurations, settings elements (groups and profiles) with similar names are replaced and with different names - added. E.g. if there is Group 1 on the server and we import a file with Group 1 and Group 2, then Group 1 will be replaced by the one in the imported file and Group 2 will be added.

You can also export/import reports (use the corresponding settings in the **Export** and **Import** dialog boxes).

Appendices

Appendix A. Operation in Central Protection Mode

Dr.Web for IBM Lotus Domino for Linux can operate in the central protection mode in a network managed by **Dr.Web Control Center**. Central protection helps automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one *anti-virus network* which security is monitored and managed from central server (**Dr.Web Control Center**) by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

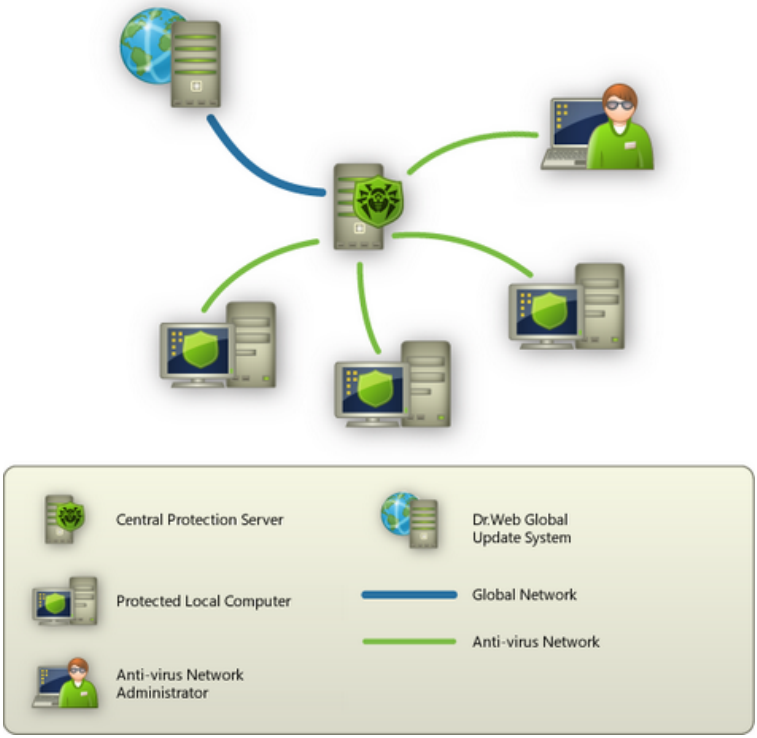
Solutions for central protection from **Doctor Web** use client-server model.

Workstations and servers are protected by *local anti-virus components* (clients; herein, **Dr.Web for IBM Lotus Domino**) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.

Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from **Dr.Web Global Update System** servers.

Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.



Operation of Dr.Web for IBM Lotus Domino in

Central Protection Mode

For operation of **Dr.Web for IBM Lotus Domino** in central protection mode, **Dr.Web Agent** is required to be installed and operate correctly on the same operating system.

Dr.Web for IBM Lotus Domino version 6.0 is compatible with **Dr.Web Agent** 6.0 or later.

Dr.Web for IBM Lotus Domino operating in the central protection mode provides the following possibilities:

- Recording the starting/stopping events of IBM Lotus Domino with the installed **Dr.Web** plug-in. Starting/stopping events display in the **Start/End** table of **Dr.Web Control Center**.
- Sending statistics for operating of **Dr.Web for IBM Lotus Domino**. The statistics is displayed in the **Statistics** and **Summary statistics** tables of **Dr.Web Control Center**.
- Sending notifications on detected viruses with information on the infection and action of **Anti-virus**. These events are displayed in the **Infection** table of **Dr.Web Control Center**.
- Registering **Dr.Web for IBM Lotus Domino Web Console** with **Dr.Web Control Center**. This allows displaying the URL for **Dr.Web for IBM Lotus Domino** administration console in the **Dr.Web Control Center Console**. URL can be set by administrator or automatically generated on the basis of options of the server document in a server's address book.

To set up URL value:

1. Set DrWebAdminURL parameter in notes.ini server file. For example:

   ```
   DrWebAdminURL=http://domino-server.domain.name/drweb/DrWebAdmin.nsf
   ```

2. Reboot Lotus Domino server.

To set up URL value without reboot of Lotus Domino server:

1. In the server console execute the following command:
   `set config DrWebAdminURL=http://domino-server.domain.name/drweb/DrWebAdmin.nsf`
2. Transfer of value URL to **Dr.Web Control Center** server will be executed within a minute.

- Updating **Dr.Web** virus databases, anti-virus engine and **Anti-spam** kernel from **Dr.Web Control Center** repositories. This action allows switching off the standard updating module of **Dr.Web IBM Lotus Domino** (**Dr.Web Updater**), which by default starts according to the schedule. In this case, the updating process starts from **Dr.Web Control Center** repositories according to its schedule.
- Using a license key file for **Dr.Web for IBM Lotus Domino** that is registered for this station at the **Dr.Web Control Center** network. To activate this function, switch the plug-in to the **Enterprise** mode. For this, do the following:
  - switch **Dr.Web Agent** to the **Enterprise** mode by specifying the **Yes** value for the **UseEnterpriseMode** parameter in the **/etc/drweb/agent.conf** configuration file.
  - execute the following command: `/etc/init.d/drweb-monitor restart`;
  - add the **DrWebEdition=Enterprise** parameter to the **notes.ini** file on the Lotus Domino server and restart the server.

In the **Enterprise** mode **Dr.Web for IBM Lotus Domino** does not use the local license key file specified in the **/etc/drweb/agent.conf** configuration file as **LicenseFile** parameter value in the **StandaloneMode** section. In the **Enterprise** mode the key file is requested from **Dr.Web Control Center**, and if it is not received, the plug-in does not perform the anti-virus check.

Appendix B. Technical Support

The **Doctor Web** technical support web page is located at http://support.drweb.com/.

If you experience problems during installation or operation of the company's products please do the following before contacting the technical support department:

- Read the **FAQ** section at http://support.drweb.com/faq/
- Visit the **Dr.Web** users forum at http://forum.drweb.com/

If the problems cannot be solved then you can contact the technical support department in one of the following ways:

- Fill out a special web-form at http://support.drweb.com/new/
- Write an e-mail message to support@drweb.com
- Telephone the technical support department in Moscow:

  +7 (495) 789-45-87

You can find the nearest office of **Doctor Web** and contact information at http://company.drweb.com/contacts/moscow