



# Dr.WEB

## for IBM Lotus Domino for Windows

### Administrator manual

Жасағаныңды

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

**Defend what you create**

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© 2017 Doctor Web. All rights reserved

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

### **Trademarks**

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk and the Dr.WEB logo 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 IBM Lotus Domino for Windows**  
**Version 11.0**  
**Administrator manual**  
**9/28/2017**

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Website: <http://www.drweb.com/>

Phone: +7 (495) 789-45-87

Refer to the official website 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

<b>Document Conventions and Abbreviations</b>	<b>6</b>
<b>1. Introduction</b>	<b>8</b>
1.1. What is Dr.Web for IBM Lotus Domino	8
1.2. Objects that are Scanned	9
1.3. License Key File	9
<b>2. Installation and Removal</b>	<b>11</b>
2.1. System Requirements	11
2.2. Compatibility	13
2.3. Installing Dr.Web for IBM Lotus Domino	13
2.3.1. Post-installation Setup	14
2.4. Removing Dr.Web for IBM Lotus Domino	15
2.4.1. Post-removal Setup	15
<b>3. Getting Started</b>	<b>17</b>
<b>3.1. Post-installation Review</b>	<b>17</b>
3.1.1. Folders and Files Created During Installation	17
3.1.2. Changes in the Lotus Domino Server Directory	18
3.1.3. Launching the Lotus Domino Server	20
3.1.4. Virus Detection Test	21
3.1.5. Spam Detection Test	22
<b>3.2. Starting the Administrator Console</b>	<b>23</b>
<b>3.3. Getting Help</b>	<b>24</b>
<b>4. Administration</b>	<b>25</b>
<b>4.1. Components of the Program</b>	<b>25</b>
<b>4.2. Groups and Profiles</b>	<b>26</b>
<b>4.3. Creating and Managing Profiles</b>	<b>26</b>
4.3.1. Setting Up Notifications	27
4.3.2. Adjusting the Monitor	28
4.3.3. Setting Up Anti-spam Filtering	30
<b>4.4. Managing Groups of Clients</b>	<b>31</b>
<b>4.5. Scanning Lotus Notes Databases</b>	<b>32</b>
<b>4.6. Managing the Quarantine</b>	<b>33</b>
<b>4.7. Managing Distribution of Reports</b>	<b>36</b>
<b>4.8. Managing the Event Log</b>	<b>38</b>



<b>4.9. Managing Filters for Databases and Email Addresses</b>	<b>40</b>
4.9.1. Reviewing the Statistics	40
4.9.2. Filtering Databases	42
4.9.3. Compiling Black and White Lists of Email Addresses	43
<b>4.10. Updating the Virus Databases</b>	<b>44</b>
<b>4.11. Configuration Export/Import</b>	<b>45</b>
<b>Appendices</b>	<b>46</b>
<b>Appendix A. Configuring Update Parameters</b>	<b>46</b>
<b>Appendix B. Frequently Asked Questions</b>	<b>47</b>
What to do when errors occur?	48
Why am I not able to open some of the databases?	49
Why is the Anti-spam component not working?	49
What should I do if the AMgr task crashes with an error?	49
How to disable virus-detection features?	50
Which databases are never scanned for viruses?	51
How to adjust the plug-in via a web interface?	52
Which files are updated by the Updater?	52
What replication types are there?	52
<b>Appendix C. Operation in Central Protection Mode</b>	<b>54</b>
<b>Appendix D. Technical Support</b>	<b>56</b>



## 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	Comment
	Warning about possible errors or important notes to which you should pay special attention.
<i>Anti-virus network</i>	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
<b>Save</b>	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
C:\Windows\ C:\Windows\	Names of files and folders, code examples.
<a href="#">Appendix A</a>	Cross-references on the document chapters or internal hyperlinks to web pages.

**The following abbreviations are used in the manual:**

Abbreviation	Description
ACL	Access Control List
CPU	Central Processing Unit
GUI	Graphical User Interface
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
NSD	Notes System Diagnostics
NSF	Notes Storage Facility (the file type for Lotus Notes and Lotus Domino databases);
NTF	Notes Template Format (templates of NSF files);
RAM	Random Access Memory
SMTP	Simple Mail Transfer Protocol



Abbreviation	Description
UNC	Universal Naming Convention
URL	Uniform Resource Locator
VDB	Virus databases
VGA	Video Graphics Array



## 1. Introduction

Thank you for purchasing Dr.Web for IBM Lotus Domino for Windows. It offers reliable protection from email 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.

### 1.1. 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 unique methods of scanning and the possibility to fully control the scanning process—all this accounts for high scanning speed and to a great extent spares system resources.

The antivirus plug-in provides scanning of email 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 also provides the facilities for administrators to control the anti-virus and anti-spam protection in large-scale Domino networks.

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

- Scan all incoming and outbound messages in realtime 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.

## 1.2. Objects that are Scanned

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

- Files attached to email messages
- Files attached to documents in databases
- OLE objects

Dr.Web for IBM Lotus Domino does not scan:

- Encrypted messages
- Documents in encrypted Lotus Domino databases
- Local database replicas located on workstations

## 1.3. 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. 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](#).



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, the warning is added to the [Event Log](#). At that, the plug-in no longer scans email messages and documents for viruses and spam, and update of the virus databases and the plug-in components is not available. Sending and receiving messages keeps working normally.

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.



## 2. Installation and Removal

The Dr.Web for IBM Lotus Domino software is distributed as a single installation file `drweb-11.0.3-av-lotus-windows.exe`. Make sure that your installation package is digitally signed by Doctor Web. For this check the **Digital signatures** tab in the **Properties** window of the installation file.

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. Extract the installation file to a folder on the local drive of the selected Domino server and make sure that it is accessible for LOCALSYSTEM user.



For proper installation and removal of Dr.Web for IBM Lotus Domino the user must be added to the group of local administrators on the computer where the Lotus Domino server is installed. When User Account Control is enabled, installation should be executed via command prompt ran with administrative privileges.

Dr.Web for IBM Lotus Domino is not compatible with other antivirus software. Installing two antivirus 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 antivirus 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](#)).

### 2.1. 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	Compatible with the i686 command system
Free RAM	512 MB or more
Disk space	750 MB or more. Temporary files created during installation will require additional disk space.
Monitor	VGA-compatible monitor is required; capability to display at least 1280 x 1024 pixels with 256 colors is recommended



## OS and software requirements

Specification	Requirement
OS	For 32-bit platforms: <ul style="list-style-type: none"><li>• Windows Server® 2003;</li><li>• Windows Server® 2003 R2;</li><li>• Windows Server® 2008;</li><li>• Windows Server® 2008 R2;</li></ul> For 64-bit platforms: <ul style="list-style-type: none"><li>• Windows Server® 2008;</li><li>• Windows Server® 2008 R2;</li><li>• Windows Server® 2012;</li><li>• Windows Server® 2012 R2;</li><li>• Windows Server® 2016.</li></ul>
File system	NTFS or FAT32
Lotus software	Lotus Domino 6.5 for Windows or later Lotus Notes 6.5 for Windows or later
Additional software	Internet Explorer 8, Mozilla Firefox 3, Opera 9 or any later versions of these web browsers (required for access to the web interface)



In case SpIDer Guard operates in the system besides Dr.Web for IBM Lotus Domino, it is necessary to add to exclusions the IBM Lotus Domino upload files in SpIDer Guard settings by adding `dwat*`, `st*.tmp` and `c*.dtf` masks to **Excluded folders and files** to enable the antivirus check by Dr.Web for 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.



## 2.2. Compatibility

Before you install Dr.Web for IBM Lotus Domino, note the following compatibility information:

1. Dr.Web for IBM Lotus Domino version 11 is only compatible with the version 11 of Dr.Web products.
2. Dr.Web for IBM Lotus Domino is incompatible with other antivirus software. Installation of multiple antivirus software on the same computer may cause system errors and loss of important data. If you have another version of Dr.Web for IBM Lotus Domino or other antivirus software installed on your computer, use the setup file or the standard tools in the operating system to remove it (see [Removing Dr.Web for IBM Lotus Domino](#)).

## 2.3. Installing Dr.Web for IBM Lotus Domino

**Before installation it is strongly recommended to:**

- install all critical updates released by Microsoft for the OS version used on your computer (all the updates are available at the company updating web-site at <http://windowsupdate.microsoft.com>)
- check the file system with the system utilities and remove the detected defects

**To install Dr.Web for IBM Lotus Domino:**

1. Shut down the Lotus Domino server.
2. Run the program's installation file `drweb-11.0.3-av-lotus-windows.exe`. An InstallShield Wizard's window will open. Click **Next**.
3. A window with the text of the License agreement will open. To continue installation you should read and accept the license by selecting **I accept these terms of the license agreement**. Click **Next**.
4. If Dr.Web Agent is installed on your computer, in the next window specify type of license. To license Dr.Web for IBM Lotus Domino you can use local key file or key file received from Dr.Web Control Center. Click **Next**.
5. If in the step 4 you selected **Use local key file** or Dr.Web Agent is not installed, specify the path to the [license key file](#). For this, click **Browse** and select the appropriate file in the file system explorer window. Click **Next** to continue.
6. A window with the list of Lotus Domino servers on which you wish to install the plug-in will open. To add a desired server to the list, click **Browse** and select the **notes.ini** file of the server. To clear the list of servers, click **Clear list**. When you finish selecting the desired servers, click **Next**.
7. The installation program will show you a list of Lotus Domino servers on which the plug-in will be installed. Click **Continue**.
8. In the next window click **Install** to begin the installation of Dr.Web for IBM Lotus Domino.



9. When the installation process ends it is recommended to perform a virus database update. For this leave the **Launch updater** check box selected and click **Finish**.
10. At the end of the installation, reboot the computer.

When installing Dr.Web for IBM Lotus Domino on several servers in one Domino domain, it is necessary to replicate the server 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](#)).

### **2.3.1. Post-installation Setup**

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 you have administrator rights for the Lotus Domino server.
2. Launch the Lotus Domino server.
3. Launch the Domino Administrator client.
4. Select **Open Server** in the **File** menu and specify the server where Dr.Web for IBM Lotus Domino is installed.
5. In the **Files** tab, select all the database patterns for Dr.Web for IBM Lotus Domino, that are located in the **DrWeb** subcatalog of the **Data** catalog: **DrWebAdmin.ntf**, **DrWebDesign.ntf**, **Quarantine.ntf**, **DrWebReports.ntf**, **DrWebHelp.ntf**, **DrWebLog.ntf** and **DrWebSpam.ntf**.
6. Right-click the selected databases and select **Sign** or click the **Sign** button 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**.



## 2.4. 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 uninstall Dr.Web for IBM Lotus Domino:

1. Shut down the Lotus Domino server.
2. Run the program installation file `drweb-11.0.3-av-lotus-windows.exe`. An InstallShield Wizard's window will open.



Alternatively you can use the **Add/Remove programs** utility in the Windows Control Panel.

3. Click the **Remove** button.
4. Once removal is complete, click **Close**.

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

### To delete the DrWebUpdate.bat program document:

1. Start the Lotus Domino server.
2. Start the Domino Administrator client.
3. Open the **Configuration** tab then select the **Programs** item under **Server**.
4. Select **DrWebUpdate.bat** in the right part of the window and delete it.

### 2.4.1. Post-removal Setup

After removing Dr.Web for IBM Lotus Domino, some email 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 email 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 email messages with the **Processing note by DrWeb for Lotus** comment in the **Failure Reason** column (see illustration below).



The screenshot shows the IBM Domino Administrator interface for the TESTLAB Domain. The main window displays a list of messages with columns for time, sender, recipient, and size. A context menu is open over the 'Release...' button, showing options such as 'Resend Selected Held Messages'. The 'Failure Reason' column for the selected messages indicates 'Processing note by DrWeb for Lotus'.

Time	Sender	Recipient	Size	Failure Reason
05/18 02:21 PM	admin@testlab.	user1@testlab.local	1,527.8	Processing note by DrWeb for Lotus
05/18 02:21 PM	admin@testlab.	user1@testlab.local	6.3	Processing note by DrWeb for Lotus
05/18 02:21 PM	admin@testlab.	user1@testlab.local	6.2	Processing note by DrWeb for Lotus
05/18 02:21 PM	admin@testlab.	user1@testlab.local	6.3	Processing note by DrWeb for Lotus

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 email 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.



## 3. Getting Started

### 3.1. Post-installation Review

Before starting the Lotus Domino server and changing the default settings of Dr.Web for IBM Lotus Domino, you can 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.

#### 3.1.1. Folders and Files Created During Installation

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

- `%PROGRAMFILES%\DrWeb for Lotus Domino\`

File name	Description
drweb32.key	License key file

- `%COMMONPROGRAMFILES%\Doctor Web\Scanning Engine\`

File name	Description
drweb32.dll	Anti-virus engine
vrcpp.dll	Anti-spam engine
dwinctl.dll	-
dwengine.exe	Dr.Web Scanning Engine service
dwsewsc.exe	-
arkdb.bin	-
dwarkapi.dll	-
dwarkdaemon.exe	-
dwqrui.exe	-

- `%ProgramData%\Doctor Web\Bases\  
(for Windows 2003 -  
%ALLUSERSPROFILE%\Application Data\Doctor Web\Bases\)`

File name	Description
*.vdb	Virus databases



- C:\Lotus\Domino\ (the path may be different depending where your Lotus Domino server is installed)

File name	Description
ndrwebmonitor.exe	The Monitor task
ndrwebscanner.exe	The Scanner task
ndrwebhook.dll	-
drwebupdate.bat	Command file for launching the Updater with command line parameters

- C:\Lotus\Domino\DATA\DRWEB (the path may be different depending where your Lotus Domino server is installed)

File name	Description
DrWebAdmin.nsf	The Administrator Console database
DrWebDesign.nsf	Service database
Quarantine.nsf	Quarantine and incidents database
DrWebReports.nsf	Reports database
DrWebHelp.nsf	Help system database
DrWebLog.nsf	Event log database
DrWebSpam.nsf	SPAM-messages database



It is not recommended to apply **Compact** utility to **drwebadmin.nsf**, **drwebdesign.nsf** and **drwebhelp.nsf** databases as it may result in errors in the plug-in work.

### 3.1.2. 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 **ndrwebhook.dll** value is added to the **EXTMGR\_ADDINS** parameter.
- The **monitor** and **scanner** tasks are added to the **ServerTasks** parameter.
- The **DrWebKey** and **DrWebBuild** parameters (whose values represent the path to the key file and the build number) are added.

If you do not want the plug-in virus detection features to automatically load when you start the Lotus Domino server, you need to delete the **ndrwebhook.dll** value from the **EXTMGR\_ADDINS** parameter and the **monitor** and **scanner** values from the **ServerTasks** parameter.



### 3.1.3. Launching the Lotus Domino Server

If Dr.Web for IBM Lotus Domino was installed successfully, you can start the Lotus Domino server (launch **nserver.exe**). 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.

```
> sh task

Task                Description
Database Server    Perform console commands
Database Server    Listen for connect requests on TCPIP
Database Server    Listen for connect requests on LAN3
Database Server    Listen for connect requests on LAN5
Database Server    Listen for connect requests on LAN4
Database Server    Load Monitor is idle
Database Server    Database Directory Manager Cache Refresher is idle
Database Server    Organization Name Cache Refresher is idle
Database Server    Idle task
Database Server    Log Purge Task is idle
Database Server    Idle task
Database Server    Perform Database Cache maintenance
Database Server    Idle task
Database Server    Shutdown Monitor
Database Server    Process Monitor
IMAP Server        Listen for connect requests on TCP Port:143
SMTP Server        Listen for connect requests on TCP Port:25
IMAP Server        Utility task
SMTP Server        Utility task
POP3 Server        Listen for connect requests on TCP Port:110
POP3 Server        Utility task
Agent Manager      Executive '1': Idle
IMAP Server        Control task
DrWeb Monitor      Idle
Process Monitor    Idle
Schedule Manager   Idle
Replicator         Idle
HTTP Server        Listen for connect requests on TCP Port:80
DrWeb Scanner      Idle
Rooms and Resources Idle
SMTP Server        Control task
POP3 Server        Control task
Directory Indexer  Idle
Indexer            Idle
Router             Idle
Calendar Connector Idle
Admin Process      Idle
Agent Manager      Idle
Event Monitor      Idle
```



### 3.1.4. Virus Detection Test

To check the functionality of the plug-in 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 email message and send it to any test email 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: Wed Jul 02 17:43:32 2016
Sent from: admin@test.com
Recipients: mail21@perf2.test.com
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!



### 3.1.5. Spam Detection Test



The Anti-spam component works 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](#)).

To test the functionality of your anti-spam component, it is recommended to use an email message with the test string.

#### To create a test spam message:

- In the Subject field specify **Vade Secure**
- Copy the following string to the body of a new email message:

```
tiUS4kVZrTfBBZXZPuLrnstNpdo8vJ-Spam-high-PQQMbQu22jePzuV8TLwVdPo81QpGXNJxRI
```

Send the message to a test email address via SMTP. The received message should contain the **[SPAM]** prefix in its subject field.



A test email should not contain signatures, attachments, or any other information, except for a subject and test string.



## 3.2. 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.

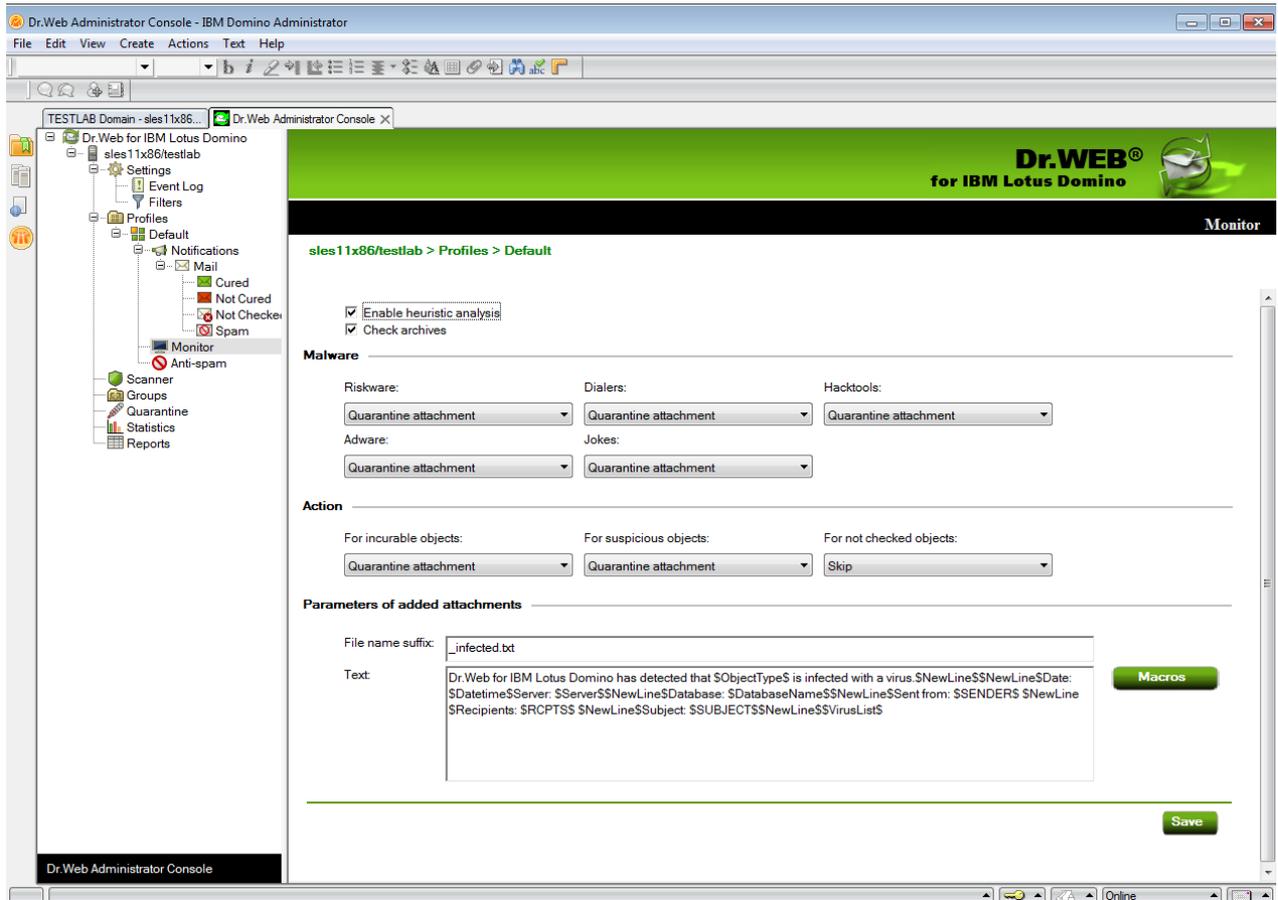
Operation of the web console requires the HTTP server task to be launched on the Lotus Domino server.

### 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. 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 you see the name and logo of Dr.Web for IBM Lotus Domino and the name of the current settings section.

### 3.3. 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.



## 4. Administration

### 4.1. 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:

- Monitor scans all incoming and outbound messages in realtime 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.
- 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.
- Quarantine is used for isolation of infected and suspicious objects. It is an NSF database (**quarantine.nsf**), which resides in the **drweb** subdirectory of the Lotus Domino **Data** folder. Access to objects in the Quarantine is performed via the Dr.Web Administrator Console database (**DrWebAdmin.nsf**).
- Automatic Updating Utility is included into the Dr.Web for IBM Lotus Domino anti-virus package and designed to automatically update the virus databases. The Automatic Updating Utility downloads copies of the virus databases via the Internet, from a local network folder or server. There are two ways to start the updater: automatic launch and command line launch (see [Updating the Virus Databases](#)).
- Anti-spam checks all messages incoming via SMTP in realtime mode as they are processed by Lotus Domino. It uses special algorithms based on the detection of spam features in email 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 Anti-spam component is only available in the "Anti-virus + Anti-spam" version (see [License Key File](#)).

- The Statistics component 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 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.

## 4.2. 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**—in this section, you can 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**—in this section, you can control the way your main virus-detection component performs
- **Anti-spam**—in this section, you can 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](#)).

## 4.3. 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:

- In the hierarchical menu, click the **Profiles** item and select **Add New** under the list of profiles to the right.
- 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: ! / \ | ; : " \* ,

- 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 want to adjust ([Notifications](#), [Monitor](#) or [Anti-spam](#)).

## 4.3.1. 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 want to set up notifications for:
  - a) **Cured**—the infected object is detected and cured
  - b) **Not Cured**—the detected object cannot be cured
  - c) **Not checked**—the message could not be checked
  - d) **Spam**—the received object is considered spam



- 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).



- To enable the sending of mail notifications for the necessary event type:
  - Select the **Send Mail notifications** check box.
- 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.
- 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.
- Edit the **Sender** field if necessary.
- When you are done, click **Save**.

### 4.3.2. 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:

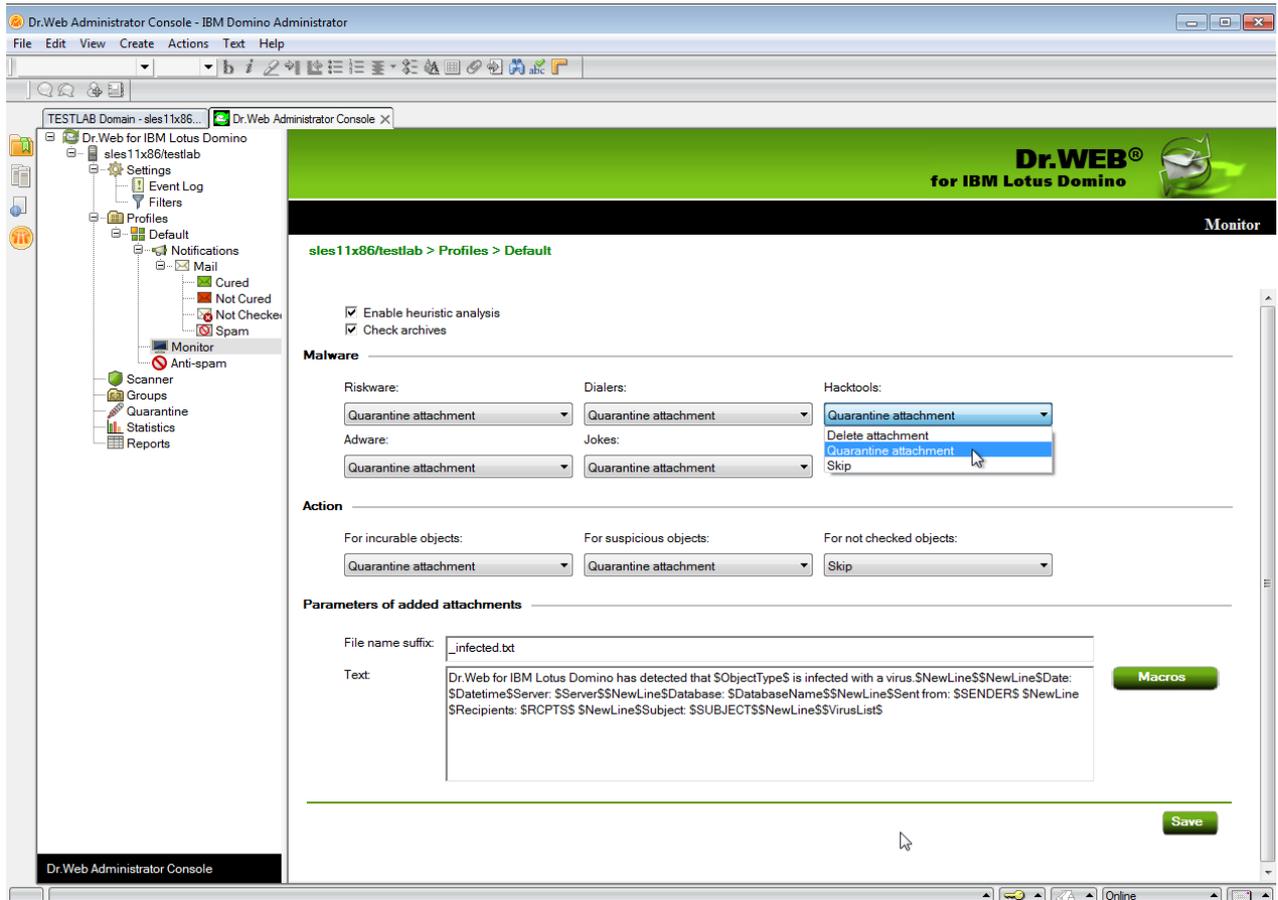
- Select the necessary profile in the hierarchical menu and click the **Monitor** item.

The illustration below 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 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 and scanning of archives in attachments as it decreases the protection level of the server greatly.



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**—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 for suspicious, incurable objects and malware).
- **Quarantine attachment**—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 email.
- **Skip**—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 email 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**.

### 4.3.3. Setting Up Anti-spam Filtering

Spam detection is performed by the Anti-spam component which analyses the contents of email 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).



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 (**C:\Program Files\DrWeb for Lotus Domino\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:
  - a) **Move to database for spam**—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).



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, automatic removal of old messages, blocking from removal. In the Lotus Notes Client, the delivery of the messages, that were wrongly classified as spam, is also provided.

- b) **Reject message**—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.



- c) **None**—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).
6. When you finish adjusting the Anti-spam component, click **Save**.



If the spam filter regards certain messages as spam by mistake, it is recommended to forward such messages to special email addresses for analysis. Please send the messages, which are wrongly regarded as spam, to [vrnospam@drweb.com](mailto:vrnospam@drweb.com), and unblocked spam messages to [vrspam@drweb.com](mailto:vrspam@drweb.com). Forward messages as attachments; do not include them to the message body.

## 4.4. Managing Groups of Clients

By default, Dr.Web for IBM Lotus Domino applies the parameters of the **Default** profile to all users. If you want to apply parameters of a different profile for certain users (see [Creating and Managing Profiles](#)), then you need to 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:

- Select the **Groups** item in the hierarchical menu and click the **Add new** button under the list of groups.
- 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: ! / \ | ; : " \* ,

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

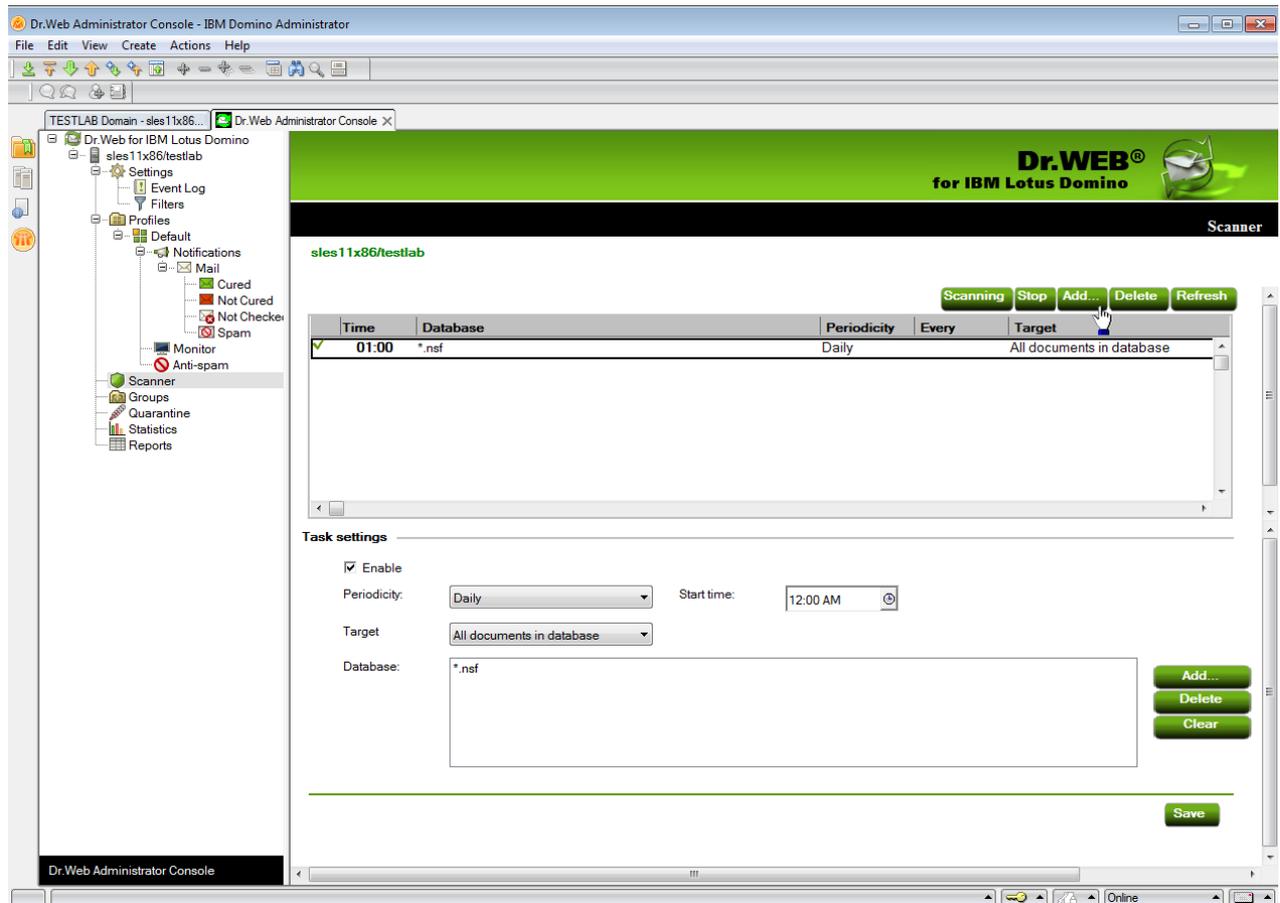


## 4.5. Scanning Lotus Notes Databases

Dr.Web for IBM Lotus Domino can check documents in certain NSF databases according to schedule. 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, where you want to check documents, 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.

You can start and stop as many scanning tasks as you want irrespectively to each other.

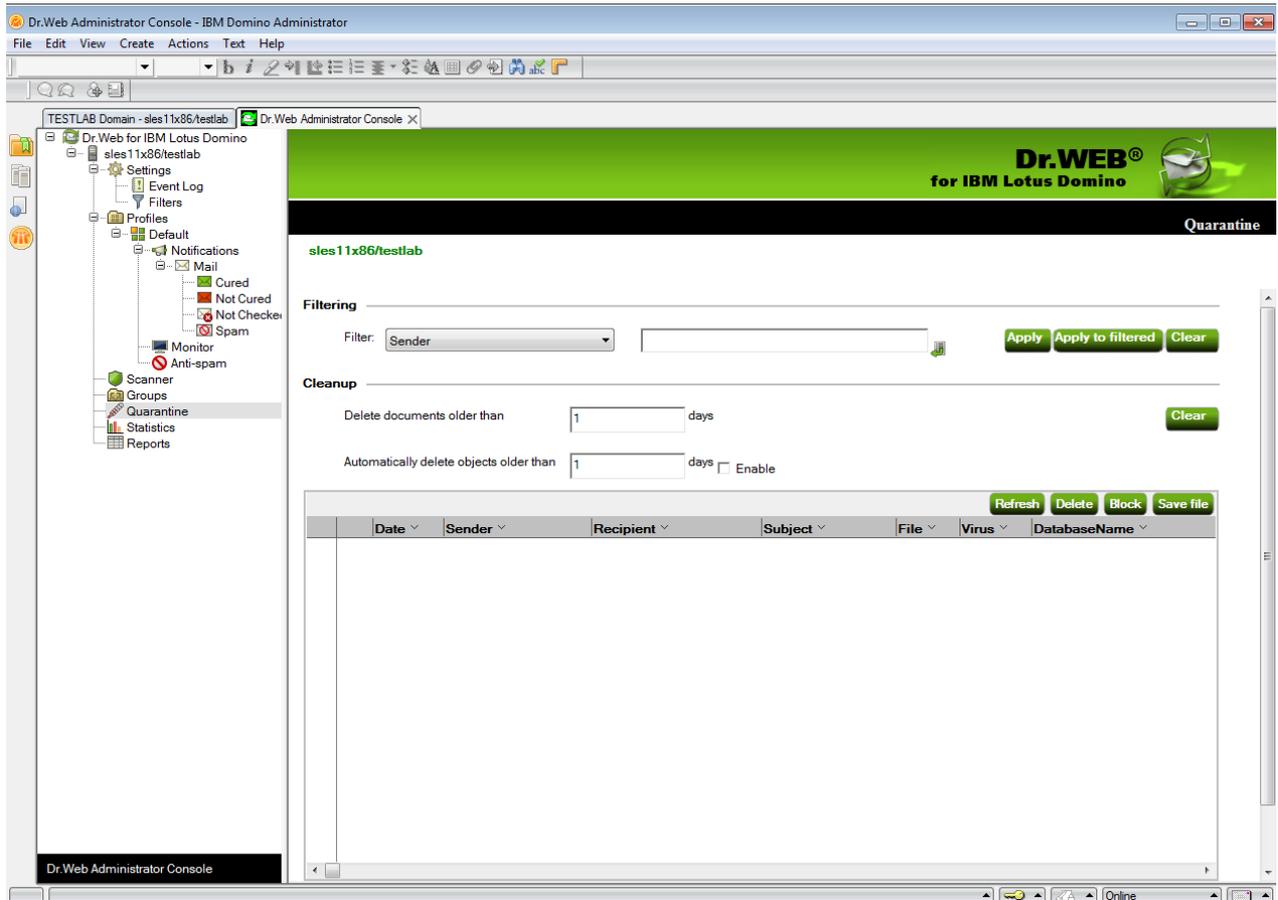
An administrator of Lotus Domino can set a size quota for every database. If, while scanning, Dr.Web for IBM Lotus Domino detects a threat in a database which quota has been exceeded, no action is applied to this threat and a corresponding message is saved to the DrWebLog database and Scanner log.

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

## 4.6. Managing the Quarantine

Quarantine is a service database (**quarantine.nsf**) that is used to isolate infected and suspicious objects. Monitor and 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) contains the list of objects in 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:

- Select the type of criteria in the **Filter** drop-down list and enter the desired value in the field to the right.
- 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 that 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 than** 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:

- Select the object.
- Click the **Save file** button to open a window with the file system tree.
- Choose the folder where you want 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.



## 4.7. 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 email 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

The screenshot shows the Dr.Web Administrator Console interface. The left sidebar contains a tree view with the following items: Settings, Event Log, Filters, Profiles (Default), Notifications, Mail (Cured, Not Cured, Not Checked, Spam), Monitor, Anti-spam, Scanner, Groups, Quarantine, Statistics, and Reports. The main content area is titled 'sles11x86/testlab' and features a 'Reports' section with a table of report types. The table has columns for Report, Recipient, Days, Schedule, and On day. Below the table are sections for 'Mail settings' (with fields for Header and Recipients), 'Manual reports' (with From and To date pickers), and 'Scheduled reports' (with an 'Enable' checkbox, 'Form for the last' days, 'Periodicity' dropdown, and 'Start time' field).

Report	Recipient	Days	Schedule	On day
✓ All Incidents	DrWeb Admin	1	Daily	
✓ Most recent viruses	DrWeb Admin	1	Daily	
✓ Incidents by recipients	DrWeb Admin	1	Daily	
✓ Spam count	DrWeb Admin	1	Daily	
✓ Who are most virused ever	DrWeb Admin	1	Daily	
✓ Who are most spammed ever	DrWeb Admin	1	Daily	

**Mail settings** **All Incidents**

Header:   
Recipients:

**Manual reports**

From:  To:

**Scheduled reports**

Enable  
Form for the last  days  
Periodicity:  Start time:

For each type of reports you can specify the subject header and recipients of the email 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 want to manually generate the selected type of reports.

**To generate reports manually:**

- Select the necessary report type.
- Specify the dates in the **From** and **To** entry fields.
- 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:**

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

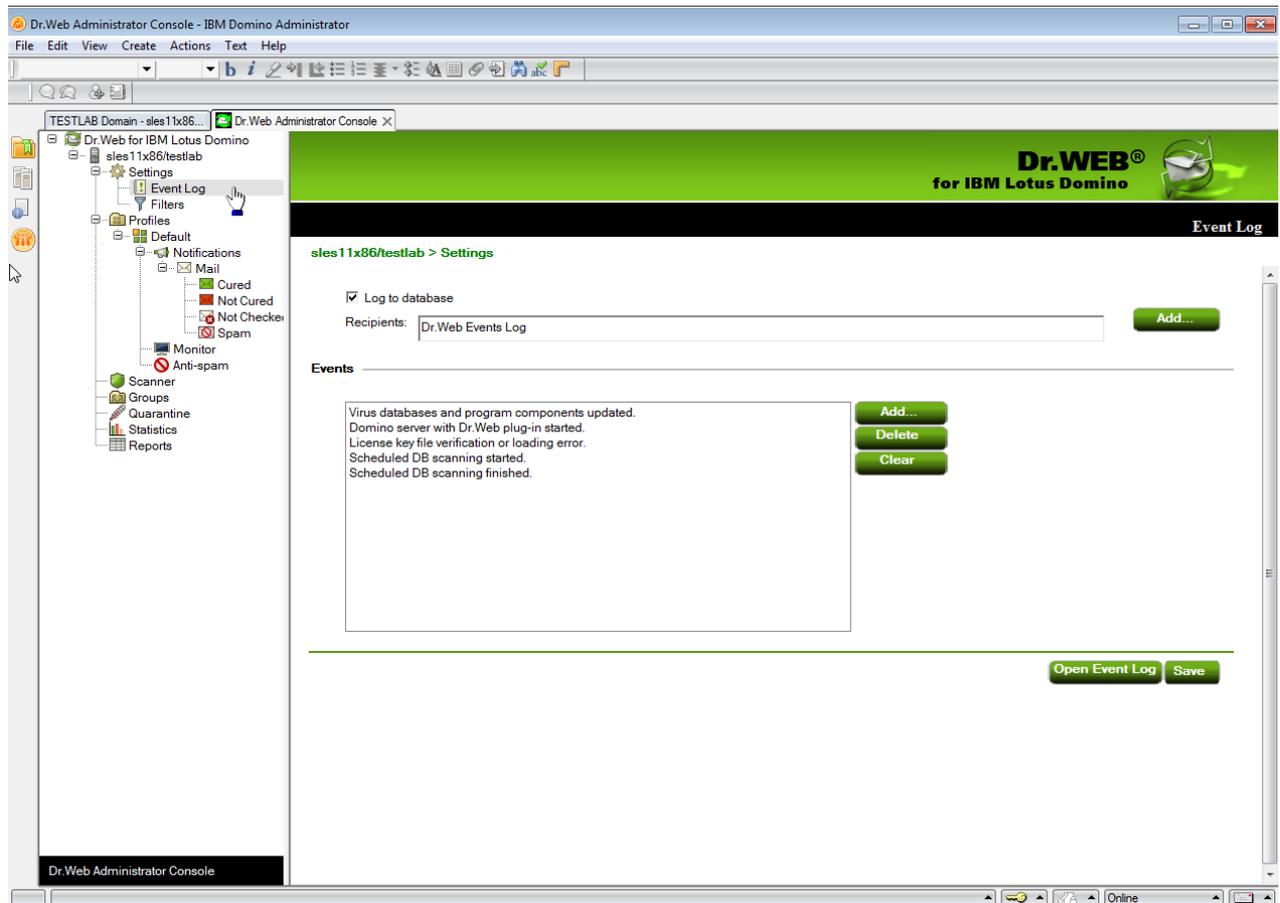


You cannot set up scheduled reports for the current day. To send a report which would include today's incidents, you have to generate it by specifying a range with the current date in the **Manual reports** group box.



## 4.8. Managing the Event Log

Logging can be useful for network administrators to keep track of various events during operation of Dr.Web for IBM Lotus Domino (it is especially useful 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.

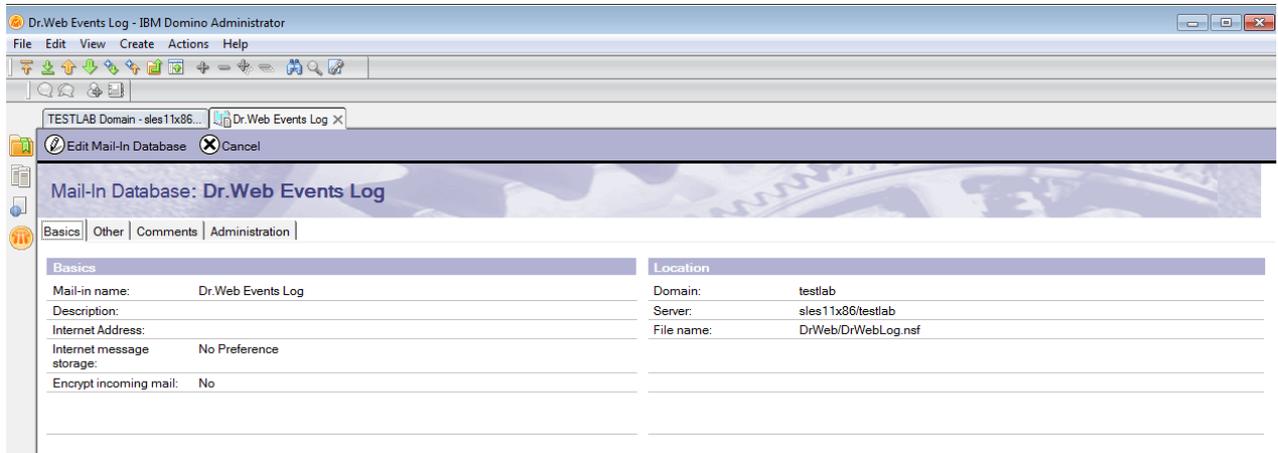


### To start and adjust logging:

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 an email address for the NSF databases where the log will be saved by adding them to the **Recipients** field via the **Add** button. Before adding a database to this field, it is necessary to specify an email address for it:
  - a) Start the Domino Administrator client.
  - b) Select the server and open the **People and Groups** tab.
  - c) Select the **Mail-In databases and resources** item.
  - d) Click **Add Mail-In Database**.



- e) Choose a name for the database, specify your email domain name and the server with the Event Log database.
- f) Specify `DrWeb/DrWebLog.nsf` in the **File Name** field.
- g) 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 want 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.



## 4.9. Managing Filters for Databases and Email 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 email addresses.

The lists can be specified manually (see corresponding tabs in the **Filters** section) or imported from a text file. For the 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 email addresses or masks, each starting on a new line, e.g.:

```
spamer1@spam.ru
*@spammers.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 want 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.

### 4.9.1. 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 (см. [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:

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

#### To cancel all filters:

- Click the **Clear** button.

If you want 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 than** 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](#)).

**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.

## 4.9.2. 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 want to be processed (databases not specified in the **Include** list WILL NOT be processed by the Monitor);
  - **Exclude**—databases which you do not want 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 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.

### 4.9.3. Compiling Black and White Lists of Email Addresses

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



All messages from the white list addresses are not be checked for spam. All messages from the black list addresses will be considered *Certainly spam* and the actions specified in the Anti-spam settings for this category will be applied to them.



You can add email 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.

## 4.10. Updating the Virus Databases

Updating of the virus definition databases is performed via the Automatic Updating Utility (Updater). The Updater launches according to schedule specified in a program document named **drwebupdate.bat** which is created in the **Domino** directory of the server address book during the installation of the Dr.Web for IBM Lotus Domino. By default, the Updater launches every 30 minutes. The program document can be edited via the Domino Administrator client.

#### To edit the updating schedule:

1. Start the Lotus Domino server.
2. Start Domino Administrator.
3. Click the **Configuration** tab and then the **Server** item in the hierarchical menu on the left.
4. Click the **Programs** item in the opened submenu and select the **drwebupdate.bat** program in the list.
5. Click the **Edit Program** button at the top of the window and make the necessary changes.

The Updater can also be launched manually in command line mode by launching the **drwebupdate.bat** file. In command line mode you can specify additional parameters (see [Appendix A. Configuring Update Parameters](#)).

If you are using a proxy server, it is necessary to adjust the Updater for operation via a proxy server. In order to do that, specify additional parameters to the **drwebupdate.bat** file (see [Appendix A. Configuring Update Parameters](#)).



## 4.11. Configuration Export/Import

With Dr.Web for IBM Lotus Domino, you can save the current configuration to a file in order to use your 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 want to import the configuration and select the **DrWeb/DrWebAdmin.nsf** on this server.
5. In the **Import configuration** group box select the settings that you want 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. Configuring Update Parameters

You can configure virus databases and Dr.Web Anti-virus components update parameters using the **drwupsrv.bat** file. This file is located in **C:\Program Files\DrWeb for Lotus Domino** installation folder.

To configure update settings, specify required parameters for **- c update** commands.

#### - c update command parameters

- **c update** command updates virus databases and Dr.Web Anti-virus components.

Parameter	Description
--type=update-revision	Type of update: <ul style="list-style-type: none"><li>• update-revision—try to update all components of the current revision to the newest if the zone differs from the local repository.</li></ul>
--disable-postupdate	Post-update is disabled. Work of update module will be stopped when the update operation has completed.
--verbosity arg	Log level: <ul style="list-style-type: none"><li>• error—standard</li><li>• info—extended</li><li>• debug.</li></ul>
--interactive	If parameter is specified, more resources will be used during execution of some operations.
-p [ --product ] arg	Apply to this product only.  If parameter is specified, all the components of the product are updated. If the parameter is not specified, all products with available updates will be updated.
-g [ --proxy ] agr	Proxy server for updating. <address>:<port>.
-u [ --user ] agr	Username for proxy server.
-k [ --password ] arg	Password for proxy server.



Example of - **c update command** for updating virus databases using proxy server:

```
-c update --type=update-revision --disable-postupdate --verbosity=debug
```

```
--interactive -p BasesForLotusPlugin -p AntispamForLotusPlugin -p LotusSetup
```

```
--proxy=192.168.134.128:808 --user=qwerty --password=qwerty
```

## Appendix B. Frequently Asked Questions

This appendix contains some frequently asked questions with answers, descriptions of problems and ways to solve them along with additional information which may be useful during operation of Dr.Web for IBM Lotus Domino.

[What to do when errors occur?](#)

[Why am I not able to open some of the databases?](#)

[Why is the Anti-spam component not working?](#)

[What should I do if the AMgr task crashes with an error?](#)

[How to disable virus-detection features?](#)

[Which databases are never scanned for viruses?](#)

[How to adjust the plug-in via a web-interface?](#)

[Which files are updated by the Updater?](#)

[What replication types are there?](#)



## What to do when errors occur?

If errors occur or Lotus Domino server crashes after installation or during operation of Dr.Web for IBM Lotus Domino, it is necessary to make sure that it was caused by the plug-in. To do this, either remove the plug-in (see [Removing Dr.Web for IBM Lotus Domino](#)) or disable its virus-detection components (see [How to disable virus-detection features?](#)). Once this is done, Dr.Web for IBM Lotus Domino will not affect the operation of Lotus Domino server, so if problems persist then they are not caused by the anti-virus plug-in. In case Dr.Web for IBM Lotus Domino did cause errors, it is necessary to collect as much information as possible before contacting technical support service (see [Technical Support](#)).

### To collect necessary information:

1. Install Dr.Web for IBM Lotus Domino if it is not installed.
2. Disable virus-detection features of the plug-in (see [How to disable virus-detection features?](#)).
3. Start the Lotus Domino server.
4. Open `notes.ini` configuration file of the Lotus Domino server.
5. Add `DrWebDebugLog=5` parameter in `notes.ini` file.
6. Save changes and close `notes.ini` file.
7. Open the Lotus Domino server console window. Run the `sh server` command and save its result.
8. Make sure that NSD (Notes System Diagnostics) launch is enabled:  
Start the Domino Administrator client and open the **Configuration** tab, then click **Server** -> **Current server document** -> **Basics** -> **Fault Recovery**. Check that the **Run NSD To Collect Diagnostic Information** parameter is enabled.
9. Stop the Lotus Domino server.
10. Enable virus-detection features of the plug-in (see [How to disable virus-detection features?](#)).
11. Start the Lotus Domino server.
12. Repeat all the actions which lead to errors or server crash as accurately as possible.

When contacting the technical support service concerning errors or server crashes caused by Dr.Web for IBM Lotus Domino, it is necessary to provide the following information:

- Last few NSD logs (which are saved to the `\Lotus\Domino\DATA\IBM_TECHNICAL_SUPPORT\` folder every time Lotus Domino server crashes).
- Dr.Web для IBM Lotus Domino event logs (which are stored in the `\Lotus\Domino\Data\DrWeb\Log` folder).
- Result of the `sh server` in the server console.
- The **System** and **Applications** sections (preferably in `.evt` format) of Windows Event Viewer.
- Details of the OS. To save information on the OS, do the following:



- Click **Start** -> **Run**
- Enter **msinfo32** and click **OK**
- Click **File** -> **Save** and save details of the OS to the nfo-file.
- Dr.Web components' versions: Monitor, Scanner, Hook, Anti-Spam, Scan Client. You can find this information:
  - In the **About Dr.Web for IBM Lotus Domino** section which can be accessed via the top item in the hierarchical menu of the Administrator Console
  - In Lotus Domino server console when server starts
  - In `ndrwebhook.dll`, `ndrwebscanner.exe`, `ndrwebmonitor.exe`, `vrcpp.dll`, `dwenine.exe` files properties, using Windows Explorer. Files location is described in [Post-installation Review](#)

Attach all required information when contacting [Dr.Web Technical Support](#).

## Why am I not able to open some of the databases?

**Quarantine.nsf**, **DrWebReports.nsf** and **DrWebDesign.nsf** are service databases of Dr.Web for IBM Lotus Domino and cannot be opened via the Lotus Notes client. Access to these databases is carried out via the Administrator Console database (**DrWebAdmin.nsf**).

## Why is the Anti-spam component not working?

If Dr.Web for IBM Lotus Domino does not detect spam and settings of the Anti-spam component are disabled, it is likely that your license key file (see [License key file](#)) does not support the Anti-spam component. To check this, open the key file (**C:\Program Files\DrWeb for Lotus Domino\drweb32.key**) with a text editor and find the following string:  
`LotusSpamFilter=No.`

If the parameter is `LotusSpamFilter=Yes` then your key file does support the Anti-spam component. In this case contact [Dr.Web Technical Support service](#).

## What should I do if the AMgr task crashes with an error?

If service databases of Dr.Web for IBM Lotus Domino (**Quarantine.nsf** and **DrWebReports.nsf**) were not signed by the server account, their agents will not be able to automatically clear incidents and objects in the Quarantine and generate reports. In this case an error message will be generated in the Lotus Domino server console window every 5 minutes:

```
AMgr: Error executing agent 'GenerateToScheduleReport' in 'drweb
\DrWebReports.nsf': Note item not found
```



### 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** and **DrWebReports.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 ID** in the **Sign Database** window and click **OK**.

## How to disable virus-detection features?

To disable virus-detection features without removing Dr.Web for IBM Lotus Domino, disable loading of the **Monitor** and **Scanner** components.

### To disable loading of the Monitor and Scanner components:

1. Open the **notes.ini** file of the Lotus Domino server where Dr.Web for IBM Lotus Domino is installed.
2. Delete the **monitor** and **scanner** tasks from the **ServerTasks** parameter.
3. Delete the **ndrwebhook.dll** value from the **EXTMGR\_ADDINS** parameter.
4. Restart the server.

### To enable loading of the Monitor and Scanner components:

1. Open the **notes.ini** file of the Lotus Domino server where Dr.Web for IBM Lotus Domino is installed.
2. Add the **monitor** and **scanner** tasks to the **ServerTasks** parameter.
3. Add the **ndrwebhook.dll** value to the **EXTMGR\_ADDINS** parameter.
4. Restart the server.



## Which databases are never scanned for viruses?

Some service databases of the Lotus Domino server are never scanned in real time because they are accessed very often and scanning them every time will lead to server overloading:

Below is the list of these service NSF databases.

- drweb\Quarantine.nsf
- drweb\DrWebDesign.nsf
- drweb\DrWebAdmin.nsf
- drweb\drwebreports.nsf
- admin4.nsf
- events4.nsf
- log.nsf
- catalog.nsf
- webadmin.nsf
- dbdirman.nsf
- names.nsf
- certlog.nsf
- clbdir.nsf
- namagent.nsf
- reports.nsf
- schema.nsf
- activity.nsf
- AgentRunner.nsf
- busytime.nsf
- certsrv.nsf
- dba4.nsf
- doladmin.nsf
- Indfr.nsf
- statrep.nsf



## How to adjust the plug-in via a web interface?

You can adjust the settings of Dr.Web for IBM Lotus Domino in a web browser via the Lotus Domino HTTP server task.

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

1. Start the Lotus Domino server.



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

## Which files are updated by the Updater?

The Updater component of Dr.Web для IBM Lotus Domino downloads and updates the following:

- Virus databases (\*.vdb)
- Anti-spam engine (**vrcpp.dll**)
- Anti-virus engine (**drweb32.dll**)
- The Updater itself (**drwebupw.exe**)

The following is NOT updated:

- Service NSF databases (**DrWebAdmin.nsf**, **Quarantine.nsf**, **DrWebReports.nsf** and **DrWebDesign.nsf**)
- Binary task files of the plug-in (**ndrwebhook.dll**, **ndrwebscanner.exe** and **ndrwebmonitor.exe**)

## What replication types are there?

There are two major types of replication:

- PULL—the server which initiates replication receives modified documents from a remote server.
- PUSH—the server which initiates replication sends modified documents to a remote server.



If Dr.Web for IBM Lotus Domino is installed on both servers which take part in the replication process, then virus detection and document curing is carried out without any problems. However, there are some peculiarities in the operation of the plug-in which should be kept in mind in cases when Dr.Web for IBM Lotus Domino is installed on one of the servers:

<b>Action</b>	<b>Task which performs replication and virus detection</b>	<b>Comments</b>
A protected server performs a PUSH-replication to an unprotected server	replica	An infected document on the protected server will be cured during replication, i.e. the unprotected server will receive a cured document. However, the document will not be cured on the protected server even after the next replication.
An unprotected server performs PUSH-replication to a protected server	nserver	During first replication, the protected server detects viruses in received documents. At the next replication, neutralized documents are replicated to the unprotected server.
A protected server performs PULL-replication from an unprotected server	replica	The protected server detects viruses in received documents and saves them after neutralization. These documents are not sent to the unprotected server even after the next replication.
An unprotected server performs PULL-replication from a protected server	nserver	If an infected document is detected on the protected server, replication will be terminated and the document will be cured. Neutralized document will be sent to the unprotected server at the next replication.



## Appendix C. Operation in Central Protection Mode

Dr.Web for IBM Lotus Domino for Windows 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 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 for Windows 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 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:

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

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

- Reboot Lotus Domino server.

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

- In the server console execute the following command:

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

- Transfer of value URL on ES 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 Dr.Web Control Center network. To activate this function, select **Use Dr.Web Control Center key file** option in [step 4](#) during installation.



If the plug-in is installed in the **Enterprise** mode, the `DrWebEdition=Enterprise.` entry will be added to the `notes.ini` file.

In the **Enterprise** mode, Dr.Web for IBM Lotus Domino does not use the local license key file that you selected at installation in, i.e. the `notes.ini` file by the `DrWebKey` parameter. In the **Enterprise** mode, privileges for scanning are verified at Dr.Web Control Center. If anti-virus scanning is not allowed, the plug-in does not perform it.



## Appendix D. Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Download and review the latest manuals and guides at <https://download.drweb.com/doc/>.
- Read the frequently asked questions at [http://support.drweb.com/show\\_faq/](http://support.drweb.com/show_faq/).
- 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 company technical support by one of the following ways:

- Fill in the web form in the corresponding section at <http://support.drweb.com/>.
- Call by phone in Moscow: +7 (495) 789-45-86.

Refer to the official website at <http://company.drweb.com/contacts/offices/> for regional and international office information of Doctor Web company.

