Dr.WEB

Mail Security Suite (IBM Lotus Domino Windows)

Administrator manual

Dr.Web Mail Security Suite (IBM Lotus Domino Windows)
Version 12.0
Administrator manual
3/18/2025

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: https://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 that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

1. About This Document

About Manual

Thank you for purchasing Dr.Web Mail Security Suite (IBM Lotus Domino Windows). This product uses the latest technologies to protect computers and data within your corporate network from email threats.

This guide is intended to help corporate network administrators install and configure Dr.Web Mail Security Suite (IBM Lotus Domino Windows) (hereinafter Dr.Web), as well as learn about its main features.

Click this link to see answers to frequently asked questions.

Document conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

Abbreviations

This manual uses the following abbreviations:

Abbreviation	Description
Dr.Web	Dr.Web Mail Security Suite (IBM Lotus Domino Windows) (an anti-virus plugin)
HTTP	stands for *Hypertext Transfer Protocol,* that is, the protocol for transferring hypertext
NSD	stands for *Notes System Diagnostics,* that is, Lotus Notes system diagnostics
NSF	stands for *Notes Storage Facility*, that is, a type of database files used in Lotus Notes and Lotus Domino
SMTP	stands for *Simple Mail Transfer Protocol,* that is, a simple protocol used to transfer emails
URL	stands for *Uniform Resource Locator* that specifies the resource, the address of a web page
OS	Operating system

2. About This Product

Dr.Web is an anti-virus plug-in that protects corporate mail system on the Lotus Domino server from viruses and spam.

Dr.Web performs the following functions:

- scanning of all incoming and outgoing messages on-the-fly (in real time);
- scheduled scanning of documents in the specified NSF (*Notes Storage Facility*) databases;
- scanning of documents as you work with them;
- scheduled scanning of replication traffic;
- scanning cluster replication traffic;
- isolation of infected and suspicious objects in the quarantine;
- filtering and blocking of incoming spam using SMTP (*Simple Mail Transfer Protocol*), as well as managing black and white lists of addresses;
- assigning users to groups to simplify management;
- sending notifications on virus events and event logging;
- virus and spam events report mail-out;
- collection of statistics;
- automated updates of virus databases and software components, scheduled or upon user's request.

Dr.Web does not support the DB2 Universal Database (DB2 UDB) software.

Product components are constantly updated, and virus databases and the spam filtering rule database are regularly updated with new entries. Continuous updating provides the essential protection for user devices, as well as applications and data.

For additional protection against unknown malware, this software uses heuristic analysis implemented in the scan engine.

The Dr.Web architecture and the ability to manage various anti-virus scanning methods ensure a high scan speed and help save the computing resources of the system. The application provides a wide range of opportunities for administrators to control spam and viruses in Domino networks of any scale.

2.1. Scanned Objects

Dr.Web scans the following objects:

- Files attached to email messages

- Files attached to documents in databases
- OLE objects

Dr.Web does not scan:

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

2.2. Program Components

Dr.Web is a complex anti-virus package which consists of several complementary components that interact with each other to ensure a high level of anti-virus protection.

- *Monitor* scans all incoming and outgoing messages in real time as they are processed by the Lotus Domino server. As soon as the message is scanned and considered safe, it is sent to the receiver. If a message contains infected or suspicious objects, the corresponding pre-defined action is applied (see Monitor Settings).
- *Scanner* periodically scans documents in the selected NSF databases. It is launched according to schedule or manually and, like Monitor, applies pre-defined actions to infected and suspicious objects (see Scanning Lotus Domino Databases).
- *Quarantine* is a place where Dr.Web isolates infected and suspicious objects (see Managing Quarantine). It is a NSF database (Quarantine.nsf), located in the `\DATA\DRWEB` directory of the Lotus Domino server. Quarantined objects can be accessed from the *Administrator Console database* (`DrWebAdmin.nsf`).
- *Automatic Updating Utility* is designed to automatically update virus databases. The Updater downloads copies of virus databases from the internet, a local network directory, or a server. There are two ways to start the updater: automatic launch and using the command line (see Updating Virus Databases).
- The *Anti-spam* component scans all incoming messages received through SMTP in real time as they are processed by the Lotus Domino server (see Anti-spam Settings). 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, a pre-defined 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 Licensing).

- The *Statistics* component saves information on the types of scanned messages and actions performed with these messages. You can view this information in order to keep track of the operation of Dr.Web (see View Statistics).
- The *Reports* component regularly sends performance reports for the application to specified addresses according to certain criteria (see Managing Reports).

- The *Event Log* component allows administrators of the Lotus Domino servers to efficiently monitor the events which occur during the operation of Dr.Web (for example, update of the virus databases, detection of viruses, configuring settings, and so on). 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 through the internal mail system of the Lotus Domino server.

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

You can control the operation of these components using the *Administrator Console*,that is, a graphical interface that can be operated either using the Lotus Notes client or a web browser (see Starting the Administrator Console).

3. Licensing

Permissions to use Dr.Web are granted by the license purchased from the Doctor Web company or from its partners. License parameters determining user rights are set in accordance with the License Agreement (see https://license.drweb.com/agreement/), which the user accepts during the installation of the product.

The license contains information on the user and the vendor as well as usage parameters of the purchased product, including:

- the list of components licensed to the user (for example, the Anti-spam component is only available in the Anti-virus + Anti-spam version);
- Dr.Web licensed period;
- availability of technical support;
- other restrictions (for example, the number of computers on which you are allowed to use Dr.Web).

For evaluation purposes, users can also activate a demo license. Having fulfilled the activation conditions, users can take advantage of full functionality of Dr.Web for the entire trial period.

Each Doctor Web product license has a unique serial number associated with a special file stored on the user computer. This file regulates the operation of product components in accordance with the license parameters and is called a *license* key file. When you activate a demo license, a special key file, named a *demo* key file, is automatically generated.

If a license or a demo period are not activated on the computer, Dr.Web components are blocked. Moreover, you will not be able to download updates for virus databases and components from the Doctor Web update servers.

3.1. License Registration and Activation

License purchasing, registration, and activation

After a license is purchased, updates to product components and virus databases are regularly downloaded from the Doctor Web update servers. If users have issues with installing or using the purchased product, they can contact technical support provided by Doctor Web or its partners.

You can purchase any Doctor Web product, as well as obtain a product serial number either via the online store or from our partners. For details on license types, visit the Doctor Web official website at https://license.drweb.com/products/biz/.

License registration is required to prove that you are a legal user of Dr.Web and to activate the functions of the anti-virus, including the regular updates of virus databases.

To activate the product, enter the serial number of the purchased license. The serial number is supplied with the product or via email when purchasing or renewing the license online. A purchased license can be activated on the Doctor Web official website at https://products.drweb.com/register/.

If you have several licenses for using Dr.Web on several servers, but choose to use the product only on one server, you can specify it and license validity period will be automatically extended.

Subsequent Registration

If a key file is lost but the existing license is not expired, you should register again by providing the personal data you specified during the previous registration. You can use a different email address. In this case, the license key file will be sent to the newly specified address.

After the key file is sent to you by email, you need to install it manually.

3.2. Obtaining Demo License

A demo period for your copy of the Dr.Web product can be obtained by sending a request through the Doctor Web official website at https://download.drweb.com/demoreq/biz/. When you select the product and fill in the registration form, you will receive an email with a serial number or a key file required to activate the demo period.

You can only obtain another demo license for the same computer after a certain time period.

3.3. Key File

User rights for the Dr.Web product are stored in the special *key file*. The file contains information on the purchased license or a demo period and regulates usage rights in accordance with it.

A *valid* key file satisfies the following criteria:

- license period is not expired,
- key file applies to all components of Dr.Web,
- integrity of the key file is not violated.

If any of the conditions is violated, the license key file becomes *invalid*, Dr.Web stops detecting malicious programs and transmits the email traffic unchanged.

The key file is digitally signed to prevent its editing. The edited key file renders invalid. We do not recommend you to open your key file in text editors so as not to change it by accident and render it invalid.

Key File Installation

Dr.Web requires a valid key file for correct operation. The path to this file is specified during the installation.

During the Dr.Web operation, the key file must be located in the default directory `C:\Program Files\DrWeb for Lotus Domino` under the name `drweb32.key`.

Plug-in components regularly check the key file for availability and validity. If no valid key file (license or demo) is found, or if the license is expired, operation of the anti-virus components is blocked until a *valid* key file is installed.

It is recommended that you keep the license key file until it expires, and use it to reinstall the product or install it on a different computer. In this case, you can use the same product serial number and customer data that you provided during the registration.

If you have a key file corresponding to the valid license for Dr.Web (for example, if you obtained the key file by email or if you want to use the program on another server), you can activate the product by specifying the path to the key file. For that, do the following:

1. Unpack the key file if archived and save it in any available directory (for instance, a local directory or removable media).

In email messages, key files are usually transferred in ZIP archives. The archive containing the key file for product activation usually named `agent.zip` (note that if the message contains several archives, it is necessary to use the `agent.zip` archive).

2. Then copy the key file to the `C:\Program Files\DrWeb for Lotus Domino` directory and rename the file to `drweb32.key` if necessary.
3. Reboot the Lotus Domino server.

3.4. Licensing Parameters

The license key file regulates the use of Dr.Web.

Licensing Parameters

1. To view licensing parameters stated in the license key file, open the file using the text editor.

The license key file is protected from editing, because editing makes it invalid. Do not save the file when you close the text editor to prevent the file from being compromised.

2. Check the following licensing parameters:

Parameter	Description
The `[Key]` group, the `Applications` parameter	It determines the components that the license owner can use.  The DominoPlugin component must be listed to use the key file with Dr.Web.
The `[Key]` group, the `Expires` parameter	Determines the license key file expiration date (`Year-Month-Day` format is used).
The `[User]` group, the `Name` parameter	Determines the license owner registration name.
The `[User]` group, the `Computers` parameter	Determines the number of users protected by the plug-in.

3. Close the file without saving.

3.5. License Update

In some cases, for example, when the license expires or security of your system is reinforced, you may need to buy a new Dr.Web license or an extended one. In this case, you should replace your license key file that is already registered in the system. You do not need to reinstall Dr.Web operation to update the license.

To replace the key file

1. To update the license, copy your new key file to the `C:\Program Files\DrWeb for Lotus Domino`.
2. Restart the Lotus Domino server, so that Dr.Web starts using the new key file.

For more information on license types, visit the Doctor Web official website at https://license.drweb.com/products/biz/.

4. Application Installation and Uninstallation

Dr.Web is supplied as an installation package `drweb-[version]-av-lotus-windows.exe`, where `[version]` is the number of the current version of the anti-virus application. Make sure that your installation package has a digital signature of Doctor Web. To do this, see the **Digital Signatures** tab in the file properties.

Before installing the application 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.

To install or uninstall Dr.Web, you need to be in the group of local administrators on the computer where the Lotus Domino server is installed. When account control is enabled, run installation with administrative privileges using the command prompt.

The application is incompatible with other anti-virus software (see Compatibility).

4.1. System Requirements

See below the Dr.Web system requirements.

Parameter	Requirements
CPU	Compatible with the i686 command system
RAM	512 MB or more
Free disk space	750 MB or more. Temporary files created during installation require additional disk space
Screen resolution	Recommended 1280 × 1024 or higher, supporting at least 256 colors
File system	NTFS or FAT32
Operating system	For 32-bit platforms: • Windows Server 2008 • Windows Server 2008 R2 For 64-bit platforms: • Windows Server 2008 • Windows Server 2008 R2

Parameter	Requirements
	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Additional software	Lotus software: • IBM Lotus Domino for Windows version 8.5 - 9.0.1 • IBM Lotus Notes for Windows version 7.0.2 - 9.0.1 • IBM Domino for Windows 10.1 • IBM Notes for Windows 10.0 • HCL Domino for Windows 11.0 • HCL Notes for Windows 11.0 Web browsers suitable for the web interface: • Internet Explorer 8 or later • Mozilla Firefox 3 or later • Opera 9 or later

Microsoft has stopped supporting SHA-1 hashing algorithm, please ensure that your operating system supports SHA-256 hashing algorithm before installing Dr.Web Security Space on Windows Vista or Windows 7. For this, install all the recommended updates listed in Windows Update section. For the detailed information, please visit Doctor Web official website.

If, in addition to the plug-in, the system has the SpIDer Guard file monitor component by Doctor Web installed, change the SpIDer Guard settings by adding the `dwat*`, `st*.tmp`, and `c*.dtf` masks to The list of excluded folders and files. In this case, the network traffic will be scanned by the Dr.Web plug-in.

Doctor Web does not guarantee the correct operation of the anti-virus application on alpha, beta, and other non-commercial versions of the Lotus Domino server.

4.2. Compatibility

Before you install Dr.Web, note the following compatibility information.

1. Dr.Web version 12.0 is only compatible with Doctor Web products version 12.0.
2. In the centralized protection mode, the plug-in is only compatible with Dr.Web Enterprise Security Suite version 12.0.
3. The application is not compatible with other anti-virus software. Installing several anti-virus products on one computer may lead to system errors and the loss of important data. If a Dr.Web version or another anti-virus software is already installed on the computer, uninstall it using the installation package or standard operating system tools (see Program Uninstallation).

4.3. Program Installation

Before Dr.Web installation it is strongly recommended that you

1. Install all critical updates released by Microsoft for the Windows version used on your computer (all the updates are available at the company update website at https://support.microsoft.com/help/12373/windows-update-faq).
2. Check the file system with the system utilities and remove the detected errors.

To install the anti-virus application

1. Shut down the Lotus Domino server.
2. Uninstall previous versions of the application and any other anti-virus software for IBM Lotus Domino on your computer using standard Windows tools.
3. Run the installation file `drweb-[version]-av-lotus-windows.exe`. Installation wizard opens. Click **Next**.
4. A window with the text of the License Agreement opens. To continue installation, read it and select **I accept the terms of the license agreement**. Click **Next**.
5. If Dr.Web Agent is installed on your computer, in the next window specify the license type. You can use the local key file. Click **Next**.
6. If in the previous step 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. Click **Next**.
7. A window with the list of Lotus Domino servers on which you wish to install the plug-in opens.

   To add the necessary 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 necessary Lotus Domino servers, click **Next**.

8. The installation program shows the list of Lotus Domino servers on which the plug-in will be installed. Click **Continue**.
9. In the next window, click **Install** to start the installation.
10. At the end of the installation, reboot the computer.

When installing Dr.Web 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` directory of the Lotus Domino server) to all other Lotus Domino servers in the domain after every installation. If you do not replicate the database, duplicates of the DrWeb Admin group will appear in the server address book and it will be impossible to send mail notifications to the application administrator.

To remove the duplicate of the DrWeb Admin group in the address directory

1. Move users from one DrWeb Admin group to another by editing the group 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 at http://www.ibm.com/developerworks/lotus/documentation/domino/).

4.3.1. Post-Installation Setup

After Dr.Web installation, it is necessary to sign new Lotus Domino server databases used by application. Otherwise, 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. Start the Lotus Domino server.
3. Start the Domino Administrator client.
4. Select **Open Server** in the **File** menu and specify the server where the application is installed.
5. On the **Files** tab, select all the Dr.Web databases located in the `\DATA\DRWEB` directory:
   - `DrWebAdmin.nsf`,
   - `DrWebDesign.nsf`,
   - `Quarantine.nsf`,
   - `DrWebReports.nsf`,
   - `DrWebHelp.nsf`,
   - `DrWebLog.nsf`,
   - `DrWebSpam.nsf`.

6. Right-click the necessary 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**.

4.3.2. Installation Check

To check if Dr.Web is correctly installed, make sure that during the installation the following directories were created and they contain all the necessary files:

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

File name	Description
`drweb32.key`	License key file

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

File name	Description
`drweb32.dll`	Scan engine
`vrcpp.dll`	Anti-spam engine
`dwinctl.dll`	Dr.Web Scanning Engine CTL
`dwengine.exe`	Dr.Web Scanning Engine service
`dwsewsc.exe`	Dr.Web Action Center Control
`arkdb.bin`	-
`dwarkapi.dll`	Dr.Web Anti-rootkit API
`dwarkdaemon.exe`	Dr.Web Anti-Rootkit Server
`dwqrui.exe`	Dr.Web Quarantine Manager

- `%ProgramData%\Doctor Web\Bases\`

File name	Description
`*.vdb`	Virus databases

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

File name	Description
`ndrwebmonitor.exe`	Monitor executable file
`ndrwebscanner.exe`	Scanner executable file

File name	Description
ndrwebhook.dll	-
drwebupdate.bat	Command file for launching the Updater with command-line parameters

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

File name	Description
DrWebAdmin.nsf	Administrator Console
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 that you use the Compact utility with the DrWebAdmin.nsf, DrWebDesign.nsf, and DrWebHelp.nsf databases because it may result in errors in the anti-virus plug-in operation.

If errors occurred during the program installation, contact the Doctor Web technical support.

4.4. Program Uninstallation

If you uninstall Dr.Web, all your groups and profiles, scanning and report settings will be lost; the quarantine and incident database (Quarantine.nsf) will be deleted.

To uninstall the anti-virus application

1. Shut down the Lotus Domino server.
2. Run the installation file drweb-[version]-av-lotus-windows.exe. Installation wizard opens.

You can launch the Installation Wizard using the **Add/Remove programs** Windows utility in the Control Panel.

3. Click **Remove**.

4. Once uninstallation is completed, click **Close**.

After uninstalling the application, you must manually delete the DrWeb Admin group in the address book of the Lotus Domino server (in the `names.nsf` database in the server's `DATA` directory) and the `DrWebUpdate.bat` document.

To delete the DrWebUpdate.bat document

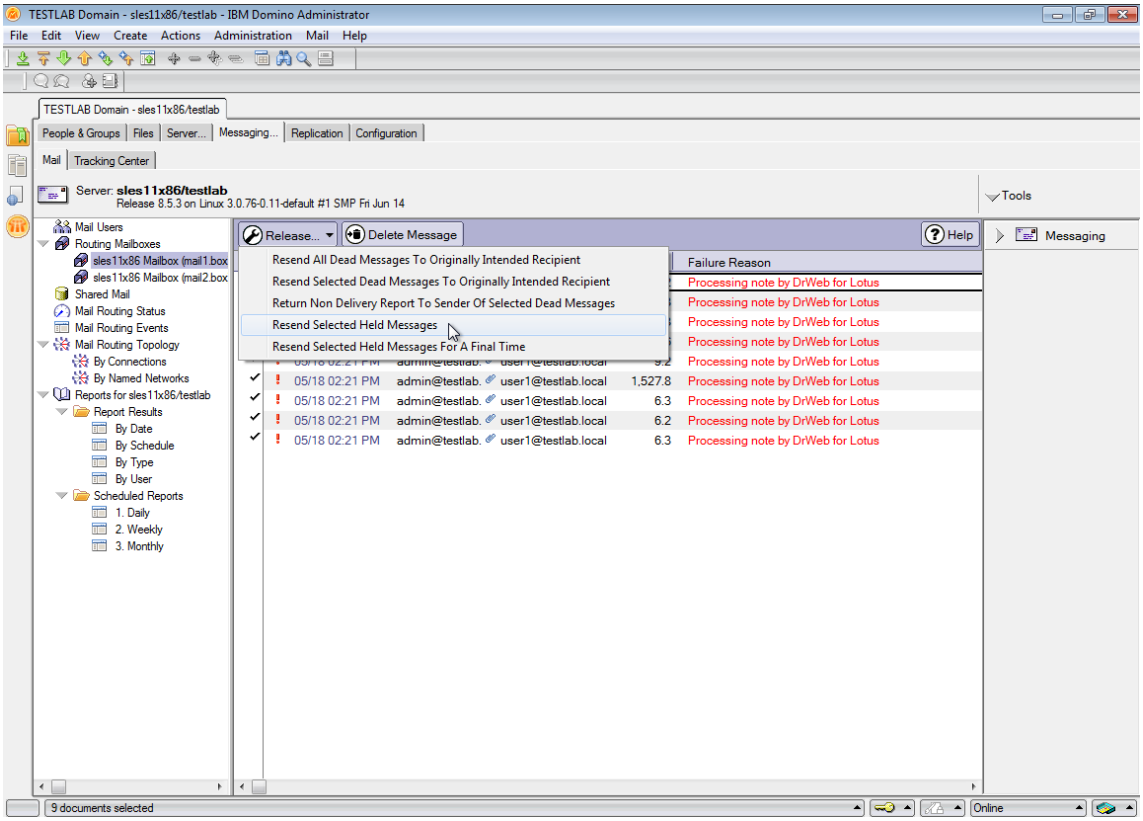
1. Start the Lotus Domino server.
2. Start the Domino Administrator client.
3. Open the **Configuration** tab, select the **Programs** item under the **Server** category.
4. Select **DrWebUpdate.bat** in the right part of the window and delete it.

4.4.1. Post-Uninstallation Setup

After uninstalling Dr.Web, some unscanned email messages may be left pending on the Lotus Domino server, because the plug-in assigns the **HOLD** status to all messages before processing.

To send pending emails to the 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 plug-in is installed.
4. Open the **Messaging** tab. Find emails with the **Processing note by DrWeb for Lotus** comment in the **Failure Reason** column in the mailboxes (under **Routing Mailboxes** in the menu on the left).



Domino Administrator client. Sending of pending messages

5. Select the messages held by the anti-virus plug-in and click the **Release** button above the list.
6. Right-click the selected messages and click **Resend Selected Held Messages**.

Released emails will be sent to the recipients and will not be scanned by the Dr.Web plug-in because it has already been uninstalled.

5. Before you start

5.1. Changes in the Lotus Domino Server Directory

During Dr.Web installation 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.

Deleting the DrWeb Admin group will lead to problems with notifications and access to databases of the plug-in.

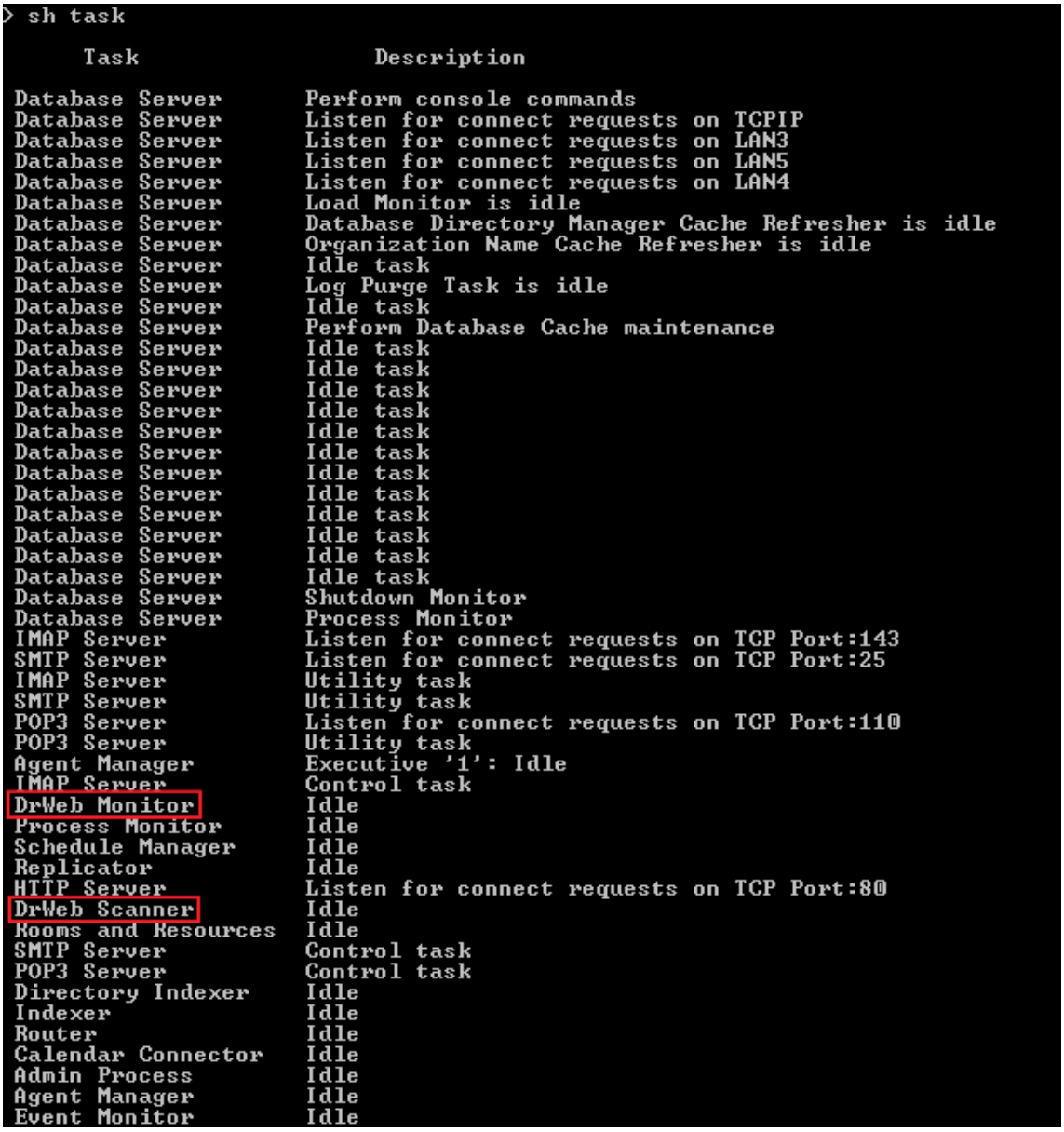
Also, the following changes are made in the `notes.ini` file:

- 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 that specify 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, delete the `ndrwebhook.dll` value from the `EXTMGR_ADDINS` parameter and the `monitor` and `scanner` values from the `ServerTasks` parameter.

5.2. Launching the Lotus Domino Server

If Dr.Web was installed successfully, start the Lotus Domino server (launch `nserver.exe`). To make sure that the Monitor and Scanner components of the plug-in are launched, use the `sh task` command.



Lotus Domino server command window with the correct result of the sh task command

5.3. Virus Detection Test

To check the functionality of Dr.Web virus detection capabilities and its default configuration, it is recommended that you 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 the 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

1. Create a text file with the following string:

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

2. Save the file with a `.com` extension (you can use any name, for example, `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 the email 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.
```

Note that it is not recommended that you use real viruses to check the functionality of an anti-virus software.

5.4. Spam Detection Test

The Anti-spam component is available in the “Anti-virus + Anti-spam” version only, that is, if you have an appropriate license.

To test the functionality of the Dr.Web anti-spam component, it is recommended that you use an email message with a test string.

To create a test spam message

1. In the subject field, specify `Test spam mail`.
2. Copy the following string to the email body:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

3. Send the message to a test email address via SMTP.

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

5.5. Starting the Administrator Console

The operation of Dr.Web is configured via Administrator Console. The console is a graphical user interface which can be launched in the Lotus Notes environment or in any supported web browser via the `DrWebAdmin.nsf` database.

For correct displaying of the Administrator Console, it is recommended that you set the resolution of your monitor to 1280 by 1024 pixels or higher (see System Requirements).

Operation of the web console requires the HTTP (*Hypertext Transfer Protocol*) server task to be launched on the Lotus Domino server.

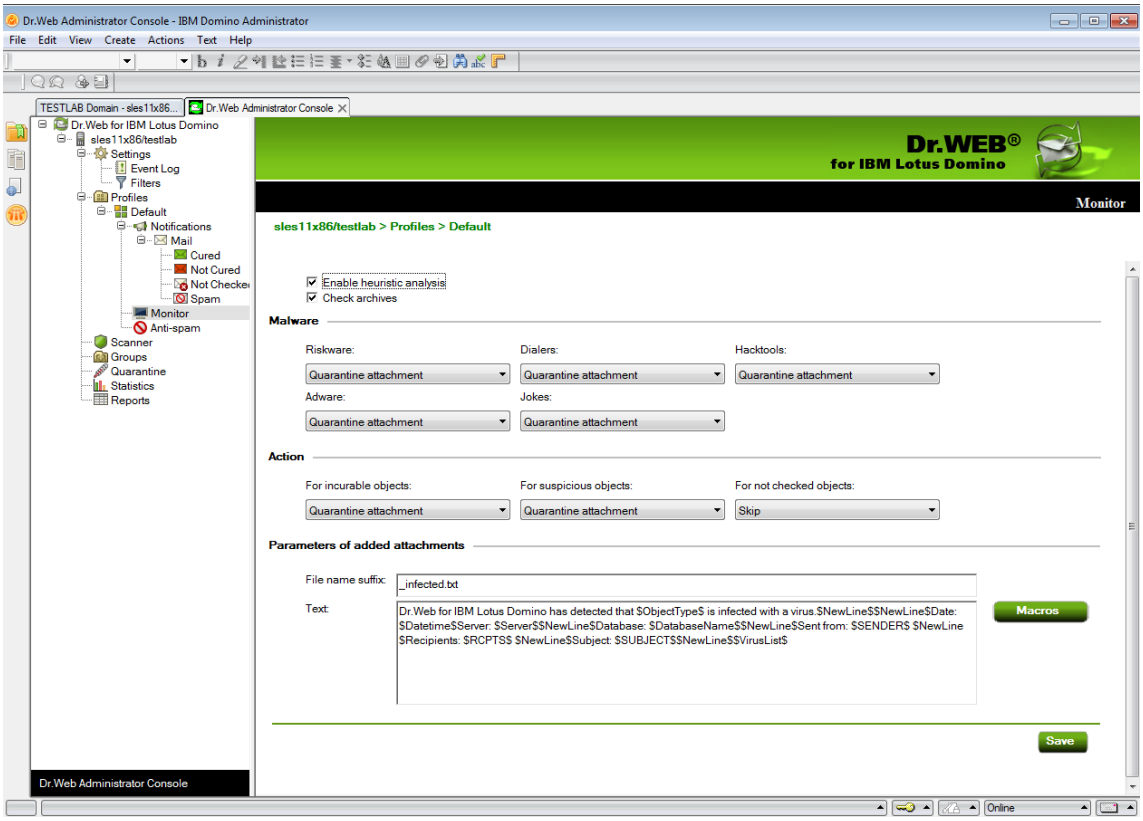
To launch the Administrator Console in Lotus Notes

1. Start the Lotus Domino server.
2. Start the Lotus Notes client software.
3. Open the **File** menu, select **Database**, and click **Open** or press CTRL+O. This will bring up the **Open Database** window opens.
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 Administrator Console database (`DrWebAdmin.nsf`) in the `\DATA\DRWEB` directory and click **Open**.

To launch the Administrator Console in a web browser

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

The Administrator Console consists of two parts. On the left is the hierarchical menu used for navigation between different sections of the program settings. On the right is the frame with the working area where the settings of the currently selected section are displayed. At the top of the frame with the working area you see the logo of the anti-virus product and the name of the selected section.



Administrator Console

5.6. Getting Help

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

To access a section in the help system depending on the context (that is, the currently selected section in the Administrator Console), press F1.

For product help, select the **Dr.Web for IBM Lotus Domino** section in the Administrator Console menu. This section contains information about the product version, key file, version numbers of software components, and the latest virus database update. This information is essential to analyze errors and issues when contacting technical support.

6. Administration

To simplify management of your Lotus Domino environment, Dr.Web allows creating groups of clients and assigning profiles to them. A profile is a set of message processing settings which determine how the protection of your Lotus Domino environment is carried out.

You can find profile settings in the **Profiles** section of the hierarchical menu. Each profile has the following subsections:

- Notifications—notification settings that keep the administrator and other users informed about various events (for example, detection of infected or suspicious messages, attempts to cure them, filtering of messages, and so on).
- Monitor—control the operation of the main virus-detection component.
- Anti-spam—the Anti-spam component settings (available in the "Anti-virus + Anti-spam" version only, that is, if you have an appropriate license).

For detailed information on creating and managing profiles, see the Creating and Managing Profiles section.

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).

6.1. Creating and Managing Profiles

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

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

It is impossible to delete the **Default** profile. The default profile parameters are set automatically for all new profiles.

To create a new profile

1. In the hierarchical menu, click the **Profiles** section and select **Add** under the list of profiles in the right part of the main frame.
2. Enter the name of the profile and click **OK**.

   A new profile will be created and a new item will appear in the **Profiles** section in the hierarchical menu.

To change the name of the profile

1. Select the profile in the hierarchical menu.

2. Enter a new value in the **Name** field and click **Save**.

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

New profile settings are similar to the default profile.

To change parameters of the new profile

1. Select the profile in the hierarchical menu.
2. Configure parameters in the Notifications, Monitor, or Anti-spam subsections.

6.1.1. Notification Settings

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, and so on).

By default, all notifications are disabled.

To configure mail notifications

1. Select the profile in the hierarchical menu.
2. Go to the **Notifications** subsection and choose the **Mail** item.
3. Select the type of events you want to configure notifications for:
   - **Cured**—the infected object is detected and cured;
   - **Not Cured**—the detected object cannot be cured;
   - **Not Checked**—the message could not be scanned;
   - **Spam**—the received email is considered as spam.
4. For each event type you can configure separate notifications for the administrator, sender and receiver. For that, switch between the corresponding tabs at the top of the frame.

5. To enable the sending of mail notifications for the necessary event type, select the **Send Mail notifications** check box.
6. If necessary, edit the template of mail notifications in the corresponding fields.
7. You can add macros to the notification body by clicking the **Macros** button and selecting the necessary ones from the list.
8. In the **Sender** field, you can specify the sender of the selected notification type.

9. The recipients of a certain type of notifications can be edited only in the **Administrator** tab. You can add users by clicking the **Add** button and selecting them in the **Select Addresses** window.
10. When you finish editing notification parameters, click **Save**.

6.1.2. Monitor Settings

The Monitor scans all incoming and outgoing messages in real-time mode as they are processed by the Lotus Domino server. Its operation parameters can be configured for different profiles to suit the needs of various groups of clients (see Groups and Profiles).

To configure parameters of the Monitor operation

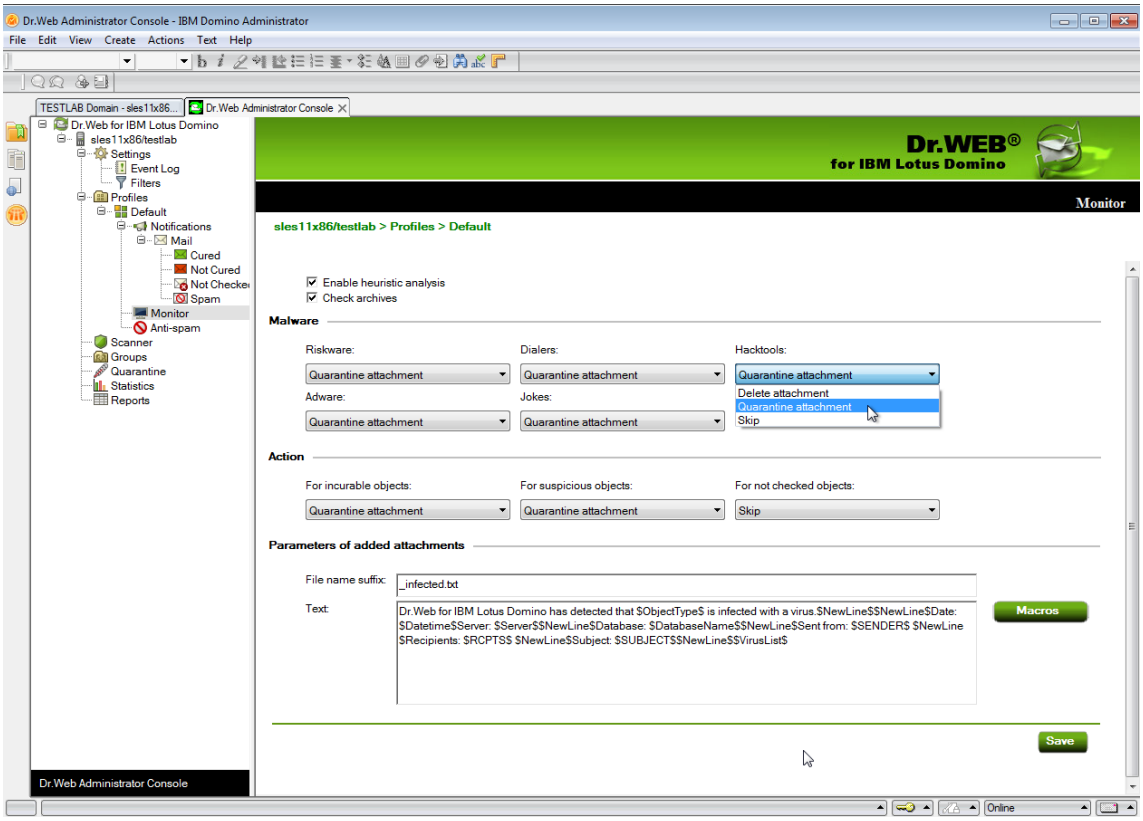
1. Select the profile in the hierarchical menu and open the **Monitor** subsection.

   By default, the heuristic analyzer and scanning of archives in attachments are enabled. This ensures 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 that you disable the heuristic analyzer and scanning of archives in attachments as it greatly decreases the protection level of the server.

2. In the **Malware** group of settings, you can choose actions for various types of potentially malicious programs. In the **Action** group of settings, you can choose actions for incurable, suspicious, and objects that cannot be scanned. For that, use the corresponding drop-down lists:
   - **Delete attachment**—the message body will be skipped and delivered to the receiver 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 only).
   - **Quarantine attachment**—the message body will be skipped and the attachment will be sent to the Quarantine database (see Managing 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 body and attachments will be delivered to the receiver without any actions applied (available for objects that cannot be scanned and malware).



Monitor frame. Selecting actions for malicious programs

3. In the **Parameters of added attachments** group of settings, you can change the suffix of the name of the text file attached to an infected email message when an action is applied to it (that is, the new file name will consist of the original name with the suffix added at the end). In the **Text** field, you can edit the text of the attached text file if necessary.
4. To add a new macro to the text file template, click the **Macros** button and select the necessary macro from the list.
5. When you finish configuring the Monitor operation parameters, click **Save**.

6.1.3. Anti-Spam Settings

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 assigned 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.

If settings in the **Anti-spam** section are unavailable, it is likely that your key file does not support scanning for spam (see Licensing Parameters). To check this, you can open the key file (`drweb32.key`) with a text editor and find the following string: `LotusSpamFilter=No`.

To configure the Anti-spam operation

1. Make sure that your version of the program includes the Anti-spam component.
2. Select the profile in the hierarchical menu and open the **Anti-spam** subsection.
3. By default, the Anti-spam component is enabled. If it is not, select the **Enable** check box at the top of the frame.
4. If you want a prefix to be added to the spam message subject, select the **Change subject** check box. You can change the prefix in the **Subject prefix** field (`[SPAM]` by default).
5. Besides adding a prefix to the subject, you can specify actions for various spam categories:
   - **Move to database for spam**—the spam message will be moved to the database specified in the **Database** field (if the specified database is not found, the spam message will be delivered to the receiver). You can also specify a folder in the database in the **Folder name** field to move the spam message to this folder (if this folder is not found in the database, the spam message will still be moved to this database but not in a specific folder).

     To store spam messages, use any of the Notes databases based on the standard mail template, for example, `Mail7.ntf`. `DrWebSpam.nsf` database is supplied with the plug-in and installed in the `\DATA\DRWEB` directory of the Lotus Domino server. It is based on a template similar to quarantine and incident databases and provides some extra functions that can be useful for spam processing, such as several types of filters, automatic removal of old messages, and locking the objects, so that they cannot be removed. The Lotus Notes Client can also deliver messages, falsely recognized as spam.

   - **Reject message**—the spam message will be received by the server and deleted without delivering it to the receiver. However, a document for this incident will be created in the `Quarantine.nsf` database.
   - **None**—no action will be applied to the message and it will be delivered to the receiver (the message subject will still be changed if the **Change subject** check box is selected).
6. When you finish configuring the Anti-spam component, click **Save**.

If Anti-spam falsely recognizes certain messages as spam, we recommend you to forward such messages to our email addresses for analysis. Send the emails falsely recognized as spam to nonspam@drweb.com and undetected spam messages to spam@drweb.com. Please forward them as attachments; do not include them in the message body.

6.2. Managing Groups of Clients

By default, Dr.Web 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), 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

1. Select the **Groups** item in the hierarchical menu and click the **Add** button under the list of groups in the main frame.
2. Choose a name for the group and click **OK**.

   A new group will be created and a new item will appear under the **Groups** section in the hierarchical menu.

To change group parameters

1. Select the group to modify in the hierarchical menu and enter a new value in the **Name** field.

   The following symbols are not allowed in the name of the group: “!”, “/”, “\”, “|”, “:”, “‘”, “*”, “,”.

3. Specify the names of 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 configuring group settings, click **Save**.

7. Program Integration

7.1. Managing Filters

Filters are used to set general restrictions for Dr.Web. They are set in the **Filters** section under the **Settings** menu. **Filters** contains two tabs.

- The **Database** tab allows you to specify the list of NSF databases that should be included or excluded from being scanned by Monitor.
- The **Anti-spam** tab allows you to specify black and white lists of email addresses.

The lists can be specified manually (in the corresponding tabs of the **Filters** subsection) 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, for example, `mail/gendir.nsf`, `trustbase/*.nsf`. For black/white anti-spam lists, the file should contain email addresses or masks, each starting from a new line, for example, `spamer1@spam.ru`, `*@spamers.ru`, `spamer2@spam.ch`.

To import data from the file to the list

1. Select the **Settings** section in the hierarchical menu and open the **Filters** subsection.
2. Click the **Import\Export** button in the lower part of the section.
3. Select the list type where you want to import the necessary data.
4. Specify the path and file name.
5. Click **Import**.

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

7.1.1. Databases Filter

A monitor is a Dr.Web component, which by default scans all the NSF databases on-the-fly, except for some Lotus Domino server service databases (see Which databases are never scanned for viruses?). Using the **Include** and **Exclude** lists in the **Database** tab of the **Filters** section under **Settings**, you can set your own restrictions for the Monitor.

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

To configure Lotus Domino database filter

1. Select the **Settings** section in the hierarchical menu and open the **Filters** subsection.
2. Select the **Databases** tab and select the **Enable** check box at the top of the tab.

3. To add a database to the list

   1.) Click **Add** next to the corresponding list:

   - **Include**—the list of databases scanned by Monitor (databases not specified in the **Include** list are not scanned).
   - **Exclude**—the list of databases excluded from the Monitor scan (databases not specified in the **Exclude** list are scanned by Monitor).

   2.) Select the database in the dialog.

   3.) Click **OK**.

   You can also list path templates, that is, paths to directories with the databases you need ending with `*.nsf`. For example, if you specify `mail\*.nsf`, all the NSF databases in the `\DATA\mail` server data directory will be added to the list (databases in subdirectories will not be added).

4. To delete a database from the list, click **Delete**.
5. To clear the list, click **Clear**.
6. Click **Save** when you finish editing the list. Changes will take effect within 1 minute after you save them.

7.1.2. Black and White Lists of Addresses

You can configure black and white lists of untrusted and trusted email addresses on the **Anti-spam** tab at the top of the **Filters** frame (the **Settings** item).

To make up address lists

1. 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 of addresses are not scanned for spam. All messages from the black list of addresses will be considered as *Certainly spam* and the actions specified in the **Anti-spam** section will be applied.

   You can add email addresses and domain names to the black and white lists using templates, that is, the "*" symbol. Templates allow you to specify ranges of addresses or domains (for example, `*@mail.com` means any address from the `mail.com` domain).

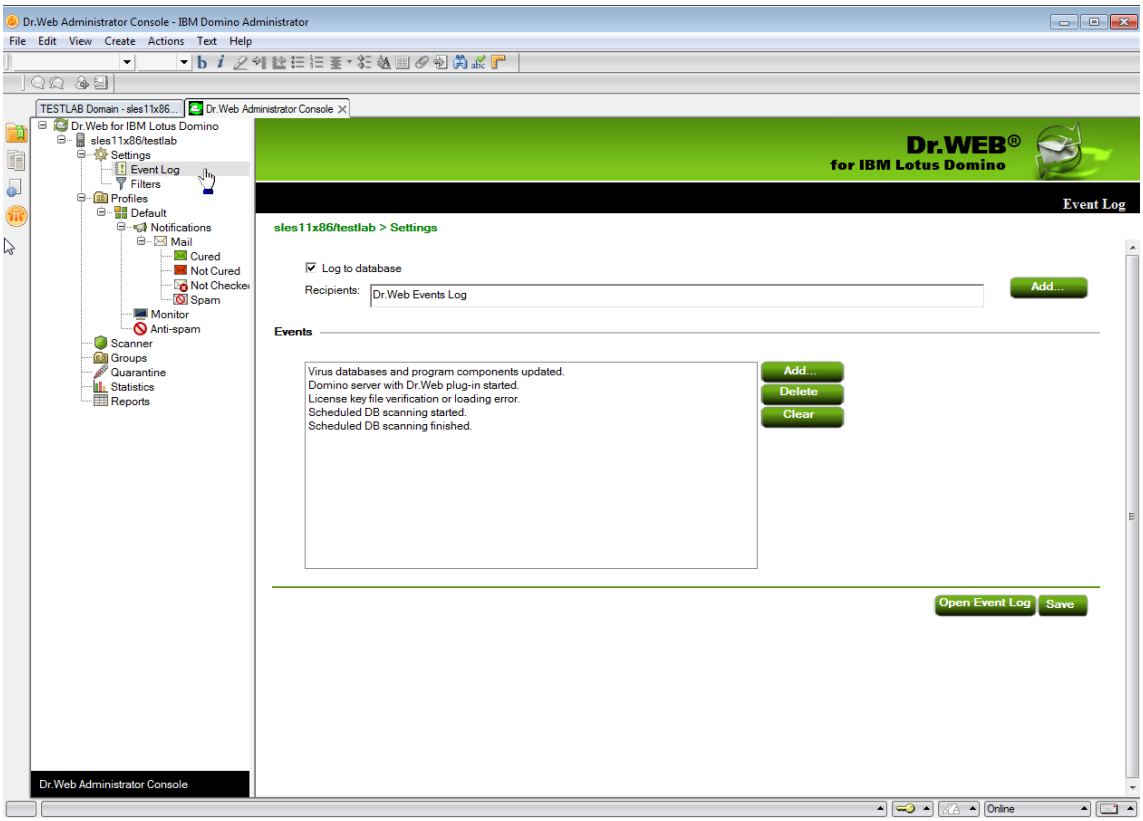
   Templates like `admin@*.com`, `*@*.com` will not work.

2. To delete an address from a list, select it and click **Delete**.
3. To clear the list, click **Clear**.

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

7.2. Managing the Event Log

Network administrators can use the event log to monitor events that occur during the operation of Dr.Web (it is especially useful if more than one Lotus Domino server is running on the network). In the **Event Log** subsection (under the **Settings** section of the menu), you can select events to be recorded in the log, as well as the database to store this information.



Administrator Console. Event Log frame

To configure logging

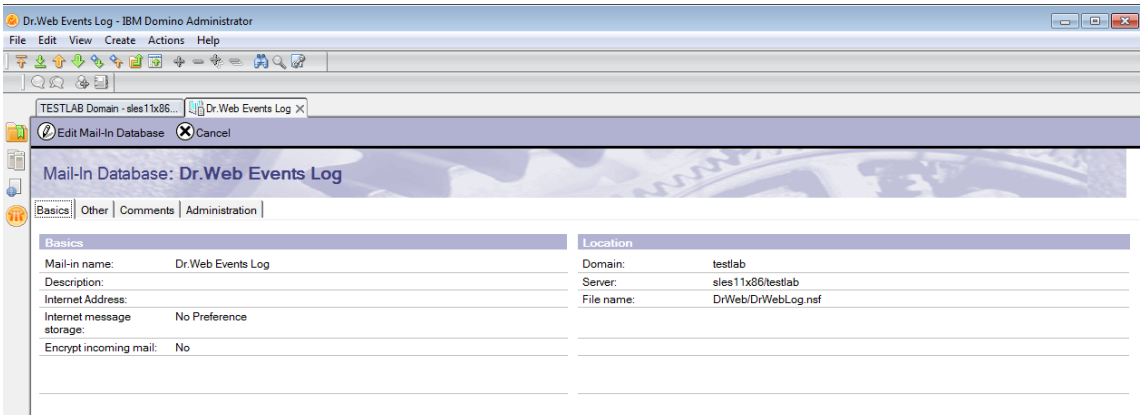
1. Select the **Settings** section in the hierarchical menu and open the **Event Log** subsection.
2. Select the **Log to database** check box to enable logging.
3. You can specify an email address for the NSF databases where the log will be saved by adding them to the **Recipients** field via the **Add** button. Before adding a database to this field, it is necessary to specify an email address for it:

   1.) Start the Domino Administrator client and select the server.

   2.) Open the **People and Groups** tab, select **Mail-In databases and resources** and click **Add Mail-In Database**.

   3.) Choose a name for the database, specify your email domain and the server.

   4.) In the **File name** field, specify `DRWEB/DrWebLog.nsf`.



Domino Administrator Client. New Shared Mail Database

5.) 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 of settings, create a list of events to be logged.
   - **Add** and **Remove** buttons allow you to edit the event list.
   - Clicking the **Clear** button will delete all events from the list.
5. Click **Save** to apply changes.

7.3. Configuration Export/Import

With Dr.Web you can save the current configuration to a file to use your settings on other servers where the plug-in is installed.

To export 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 **Export**.
4. In the opened dialog window, select the **Enable** check box and specify the path and the file name of the output file in the **Export configuration** section.
5. Click **Export**.

To import 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 **Import**.
4. Select the server where you want to import the configuration and select the `DRWEB/DrWebAdmin.nsf` database on this server.
5. In the **Import configuration** group, select settings that you want to import and the XML file with the configuration.
6. Click **Import**.

When importing configurations, settings of groups and profiles with similar names are replaced and new settings are added. For example, if there is Group 1 on the server and we import a file with Group 1 and Group 2, 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 windows).

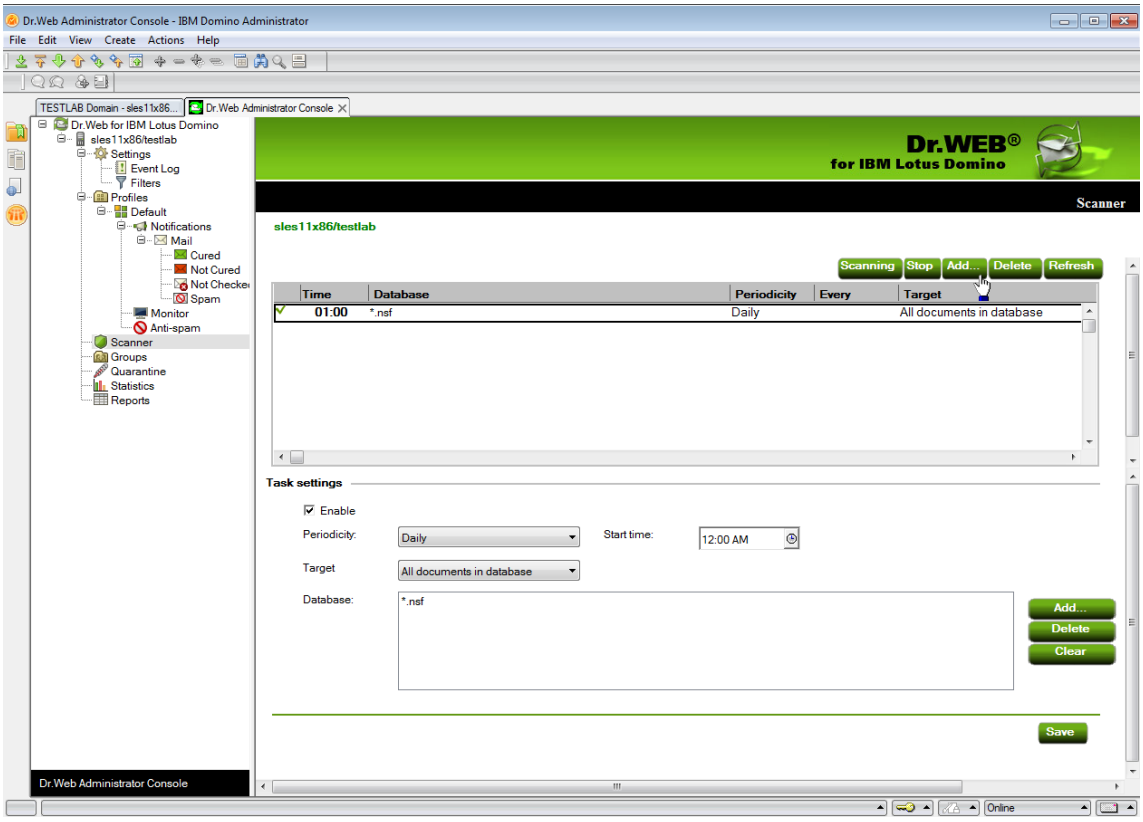
8. Anti-Virus Scan

8.1. Scanning Lotus Domino Databases

Dr.Web can perform anti-virus scan of documents in selected NSF databases according to schedule. The schedule is formed by tasks which determine the period, time, and day of scanning, as well as the databases which should be scanned.

To create a task for the anti-virus scan

1. Select the **Scanner** section in the hierarchical menu and click the **Add** button under the list of tasks in the top part of the **Scanner** frame. A new task with default values will appear in the list.



Administrator Console. Scanner frame

2. Select the created task and specify the frequency, day, and time of the scan start (the lower part of the **Scanner** frame).
3. Using the **Add** button, add the databases you need to scan to the list. For each directory, you can either select individual databases or add all the databases from this directory to the list by selecting ***.nsf**.
4. In the **Objects** drop-down menu, you can choose to scan all the objects in the specified databases or only those that have been created or changed since the last anti-virus scan (that is, perform an incremental scan that can save significant time and server computing 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 databases, the document will never be rescanned during the incremental scanning unless it is modified. Therefore, it is recommended that you periodically update virus databases 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, the Scanner starts to scan documents in the specified databases.

You can start and stop as many scanning tasks as you want independently of each other.

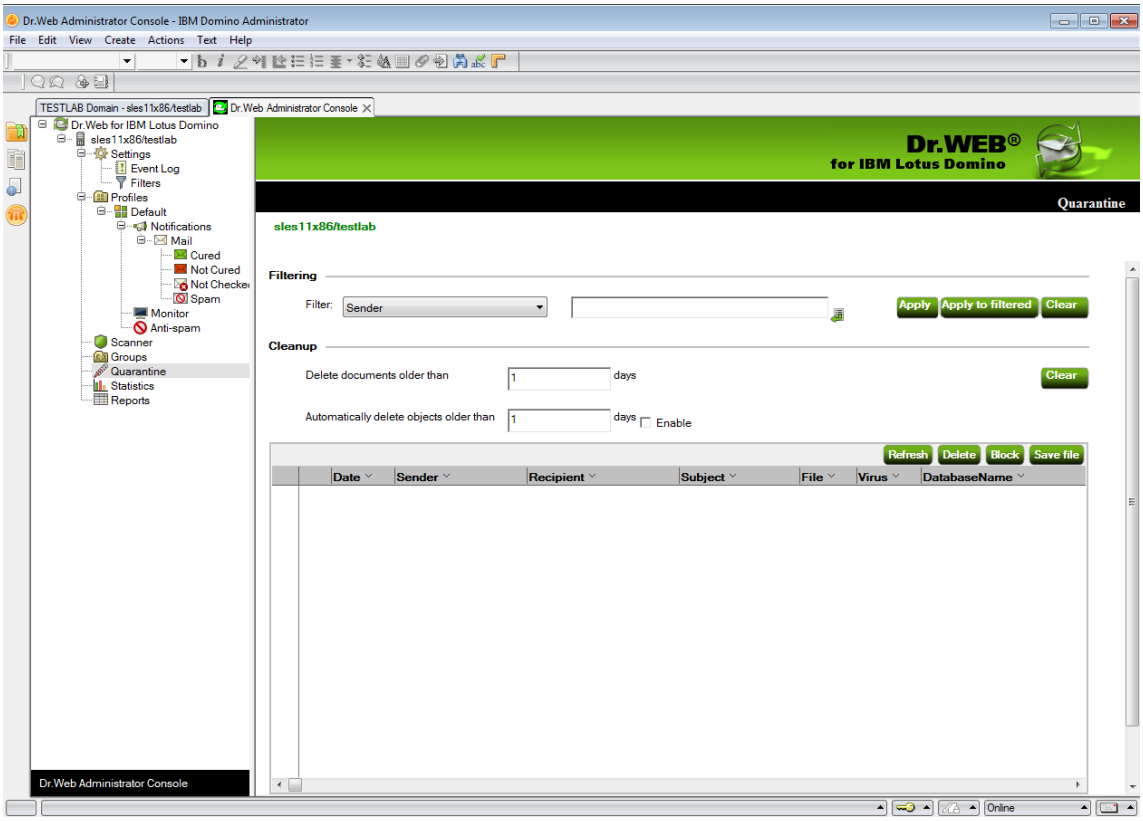
The Lotus Domino administrator can set a quota for the size of every database for a specific user. If, while scanning, the plug-in scans the database which quota has been exceeded and detects a threat, no action is applied to this threat and a corresponding message is saved to the DrWebLog database and the Scanner log.

When you finish editing scanning tasks, click **Save**.

8.2. Managing 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 database in the form of documents when the **Quarantine attachment** action is applied to them.

The **Quarantine** frame contains the list of objects in quarantine and a number of settings for configuring this list and managing documents in the `Quarantine.nsf` database. To sort the list according to certain criteria, click the headings of the corresponding columns.



Administrator Console. Quarantine frame

In the **Filtering** group of settings, you can filter the entries on the list to display documents with a specific date, virus type, and so on.

To filter the list

1. Select the type of filter in the **Filter** drop-down list and enter the value in the field to the right.
2. Click **Apply** or **Apply to filtered**:
   - **Apply**—filters all documents in Quarantine;
   - **Apply to filtered**—filters listed documents only (if the list has already been filtered).

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

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

To clear the list

1. Set the number of days in the **Delete documents older than** field.
2. Click **Clear**.

To delete all documents from the Quarantine database, you can specify `0` days in the **Cleanup** group of settings. 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.

To delete older objects automatically

1. Set the number of days in the **Automatically delete objects older than** field.
2. Select the **Enable** check box.

The Automatically Delete Objects agent removes documents from Quarantine 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 documents at http://www.ibm.com/developerworks/lotus/documentation/domino/).

To delete a document from the Quarantine

1. Select the document from the list.
2. Click **Delete**.

To save the object moved to 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 directory where you want to save the object to and click **OK**.

To block removing the document from Quarantine

1. Select the document in the list.
2. Click **Block**.

   Clicking it again will unlock the selected document, allowing you to remove it.

The Quarantine list is automatically updated every 12 hours, but you can update it manually 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.

8.3. Viewing Statistics

The Statistics component collects information about all the events concerning the Dr.Web main functions (detection of infected objects, application of actions to them, spam filtering, and so

on). To view this information, select the **Statistics** section in the hierarchical menu. The section is divided into two tabs.

- The **Statistics** tab contains a brief summary of scanned objects, infected objects, cured objects, and so on (the statistics is updated upon every event, but no more frequently than once a minute).
- The **Incidents** tab contains a list of documents with information about the events which occurred during application operation (virus or spam detection, and so on). Reports are generated according to these documents (see Managing Reports).

Settings in the **Incidents** tab are similar to those in the **Quarantine** section (see Managing Quarantine). You can also filter documents in the list to view only the documents with a certain date, virus type, and so on.

To filter the documents

1. Select the type of filter in the **Filter** drop-down list and enter the value in the field to the right.
2. Click **Apply** or **Apply to filtered**:
   - **Apply**—filters all documents of Statistics;
   - **Apply to filtered**—filters listed documents only (if the list has already been filtered).

To delete a document from the list of incidents

1. Select the document in the list.
2. Click **Delete**.

To delete old documents from the list of incidents

1. Set the number of days in the **Cleanup** group of settings.
2. Click **Clear**.

In the **Cleanup** group of settings, you can also set the time period, after which objects quarantined for more than a certain number of days will be automatically removed. Automatic removal is performed by the Automatically Delete Objects agent in the `Quarantine.nsf` database. By default, this agent runs on the server daily at 01:30. You can change its launch options using standard Lotus Domino tools (see IBM Lotus Domino Documentation).

To block removing the document from Quarantine

1. Select the document in the list.
2. Click **Block**.

   Clicking it again will unlock the selected document, allowing you to remove it.

The list is automatically updated every 12 hours, but you can update it manually by clicking the **Refresh** button.

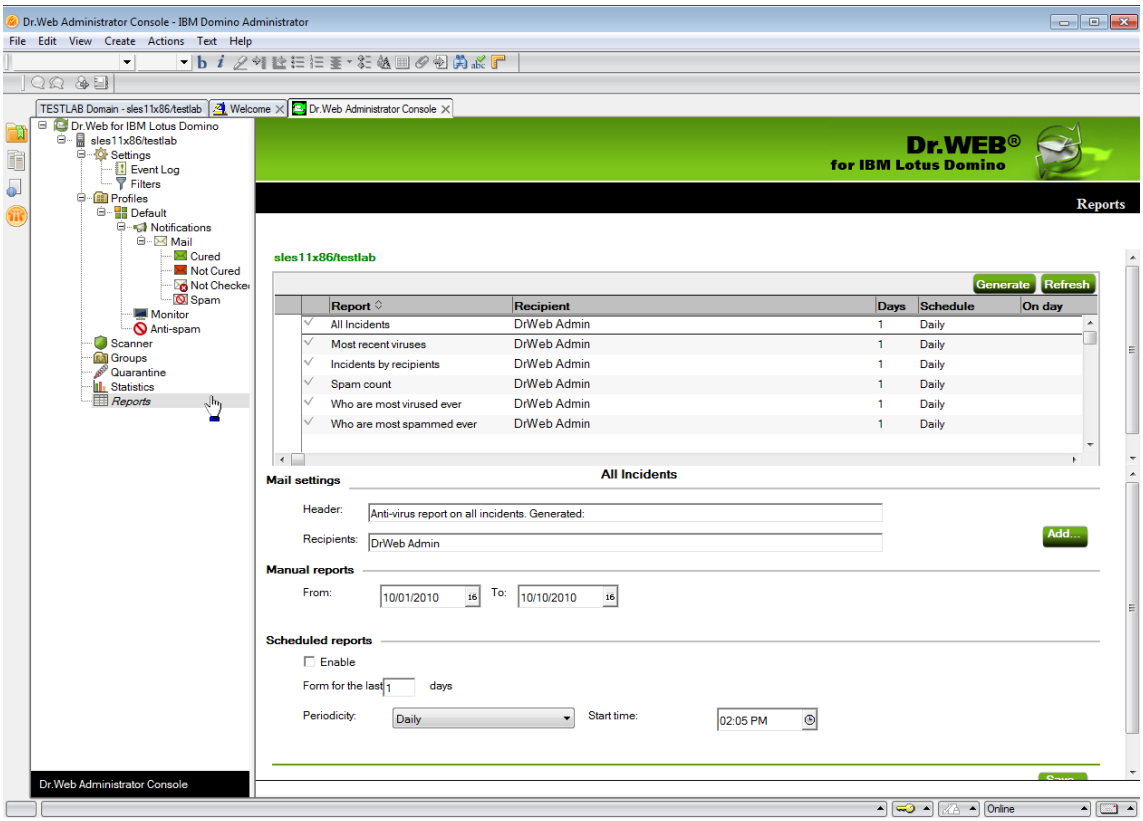
This process takes some time (up to a few minutes) depending on the amount of objects in the incidents list.

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

9. Managing Reports

Dr.Web can create reports on the operation of the anti-virus plug-in and send them to the specified addresses as HTML attachments. The reports are based on the list of documents in the **Incidents** tab of the **Statistics** section.

You can customize the distribution of reports in the **Reports** section.



Administrator Console. Reports frame

At the top of the **Reports** frame is a list of six report types which you can configure:

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

In the **Mail settings** group of settings, for each type of reports, you can specify the subject header and recipients of the email reports in the **Header** and **Recipients** entry fields under the list of report types. As recipients, you can specify a client, several clients, or a Lotus Domino server client group. Click **Add** and select the recipients in the dialog.

In the **Manual reports** group of settings, you can manage the dates of incidents for which you want 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 of settings, you can specify the schedule for automatic distribution of the selected report type.

To enable scheduled distribution of reports

1. Select the **Enable** check box.
2. Specify the number of days (preceding the current day), for which you want to generate the reports (that is, if you specify "1", only yesterday's incidents will be in the report; if "2", then the report will contain incidents that occurred in the last two days; and so on).
3. Specify the frequency, date, and time for report mail-out.
4. Click **Save**.

You cannot schedule the automatic mailout of reports for incidents that occurred during the current day. If you want to send a report with incidents for today, generate it in the **Manual reports** group of settings and specify a range with today's date.

10. Updating Virus Databases

Dr.Web uses virus databases to detect malicious software. These databases contain details and signatures for all viruses and malicious programs known at the moment of the plug-in release. However modern computer viruses are characterized by the high-speed evolvement and modification. More than that, within several days and sometimes hours, new viruses emerge which can infect millions of computers around the world. To mitigate the risk of infection during the licensed period, Doctor Web provides you with regular updates to virus databases and plug-in components. Virus databases are considered outdated after 24 hours since the last successful update.

The Dr.Web virus databases are updated via the Updater module. The Updater launches according to schedule specified in the `drwebupdate.bat` document which is created in the `Domino` directory of the server address book during the installation. By default, the Updater launches every 30 minutes. The `drwebupdate.bat` can be edited via the Domino Administrator client.

To change the update schedule

1. Start the Lotus Domino server.
2. Start the Domino Administrator client.
3. Click the **Configuration** tab and select 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 the command line mode using the `thedrwebupdate.bat` file. In the command line mode, you can specify additional parameters (see Configuring Update Parameters).

If you are using a proxy server, configure Updater for operation via a proxy server. For that, add corresponding parameters to the `drwebupdate.bat` file (see Configuring Update Parameters).

10.1. Configuring Update Parameters

You can configure virus databases and Dr.Web components update parameters using the `C:\Program Files\DrWeb for Lotus Domino\drwupsrv.bat` file.

The `-c update` command updates virus databases and anti-virus application components. To configure update settings, specify required parameters for `-c update` commands.

Parameters for the –c update command

Parameter	Description
`--type=update-revision`	The update type `update-revision` updates all components of the current revisions if the zone differs from the local repository.
`--disable-postupdate`	Post-update is disabled. Operation of the update module will be stopped when the update operation is completed.
`--verbosity arg`	Log level: • `error`—standard • `info`—extended • `debug`.
`--interactive`	If the parameter is specified, more resources will be used during execution of some commands.
`-p [ --product ] arg`	Apply to this product only. If parameter is specified, all 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. Proxy server for updating in the *<address>:<port>* format.
`-u [ --user ] agr`	Username for proxy server.
`-k [ --password ] arg`	Password for proxy server.

Example of the `-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
```

11. Operation in Centralized Protection Mode

Dr.Web can operate in the centralized protection mode in a network managed by Dr.Web Control Center. Centralized 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 the centralized protection 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

Doctor Web solutions for central anti-virus protection use a client-server model.

Workstations or servers are protected from security breaches and spam by *local anti-virus components* (clients) that ensure anti-virus protection and facilitate the connection to the centralized protection server.

The stream of instructions, data, and statistics in the anti-virus network also goes via the centralized protection server. All the 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 centralized protection server from the servers of Dr.Web Global Update System.

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

Dr.Web in the centralized protection mode

Dr.Web Agent needs to be installed and operate correctly, so that the anti-virus plug-in could operate in the centralized protection mode.

In the centralized protection mode, Dr.Web has the following options:

- recording the startup/termination events of IBM Lotus Domino with the installed Dr.Web plug-in. The startup/termination events are displayed in the **Start/End** table of Dr.Web Control Center;

- sending the plug-in statistics. 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 applied action. These events are displayed in the **Infection** table of Dr.Web Control Center;
- sending URL to the web console of the Dr.Web administrator to Dr.Web Control Center. This allows displaying the URL via the console for managing the anti-virus plug-in on the specific IBM Lotus Domino server. A URL can be set by the system administrator or automatically generated based on the settings of the server document in the address book of the Lotus Domino server.
- updating Dr.Web virus databases, scan engine, and Anti-spam databases from Dr.Web Control Center repositories. This action allows you to disable the standard Dr.Web Updater, which by default performs scheduled updates. In this case, the components will be scheduled to update by Dr.Web Control Center and via its repository;
- using the Dr.Web license key file registered for this station at the Dr.Web Control Center network. To activate this function, select **Use Dr.Web Control Center key file** option in step 5 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 will not use the local key file selected during installation and specified in the `notes.ini` file by the `DrWebKey` parameter. In the **Enterprise** mode, privileges for scanning are verified at the Dr.Web Control Center. If anti-virus scanning is not allowed, the plug-in does not perform it.

To set the URL value

1. Set the DrWebAdminURL parameter in the `notes.ini` server file. For example,

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

2. Reboot the Lotus Domino server.

To set the parameter value without rebooting the Lotus Domino server

- In the server console, execute the following command:

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

Transfer of the value to the Dr.Web Control Center will be executed within a minute.

12. Frequently Asked Questions

This section contains 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.

12.1. What to do when errors occur?

If errors occur or Lotus Domino server crashes after installation or during the operation of Dr.Web, make sure the error was caused by the plug-in. To do this, uninstall the plug-in or disable its components (see How to disable virus-detection features?). Once this is done, the plug-in will not affect the operation of the Lotus Domino server. If the issue persists, it will mean it was not caused by the plug-in. However, if Dr.Web did cause the errors, you need to collect as much information as possible before contacting technical support (see technical support).

To collect the necessary information

1. Install Dr.Web if it has been uninstalled.
2. Disable virus-detection features of the plug-in (see How can I disable virus detection?).
3. Open the `notes.ini` configuration file of the Lotus Domino server.
4. Add `DrWebDebugLog=5` parameter in the `notes.ini` file.
5. Start the Lotus Domino server.
6. Open the Lotus Domino server console window. Run the `sh server` command and save its result.
7. Make sure that the NSD (*Notes System Diagnostics*) launch is enabled:

1.) Start the Domino Administrator client and open the **Configuration** tab.

2.) Select **Server** → **Current server document** → **Basics** → **Fault Recovery**.

3.) Make sure that the **Run NSD To Collect Diagnostic Information** parameter is enabled.

8. Stop the Lotus Domino server.
9. Enable loading of the plug-in (see How can I disable virus detection?).
10. Start the Lotus Domino server.
11. Repeat all the actions which lead to errors or server crash as accurately as possible.

When contacting technical support concerning errors or server crashes caused by the plug-in, it is necessary to provide the following information:

- the latest NSD logs (saved to the `\Lotus\Domino\DATA\IBM_TECHNICAL_SUPPORT\` directory every time Lotus Domino server crashes);
- plug-in logs (saved to `\Lotus\Domino\DATA\DRWEB\Log`);
- result of the `sh server` command in the server console;
- the **System** and **Applications** sections (preferably in the `.evt` format) of Windows Event Viewer;
- the OS data. To save information on the OS, do the following:
  1.) Click **Start** → **Run**.
  2.) Enter `msinfo32` and click **OK**.
  3.) Click **File** → **Save** and save details of the OS to the NFO file.
- versions of plug-in components: Monitor, Scanner, Hook, Anti-spam, Scan Client. You can find this information:
  - in the **About Dr.Web for IBM Lotus Domino** section that can be accessed from the top item in the hierarchical menu of the Administrator Console;
  - in the Lotus Domino server console, when the server launches;
  - in the `ndrwebhook.dll`, `ndrwebscanner.exe`, `ndrwebmonitor.exe`, `vrcpp.dll`, and the `dwenine.exe` files that can be accessed via the Windows Explorer. See the location of files in the Installation Check section.

Attach all required information when contacting Doctor Web technical support.

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

The `Quarantine.nsf`, `DrWebReports.nsf`, and `DrWebDesign.nsf` are service databases that cannot be opened via the Lotus Notes client. Access to these databases is carried out via the interface of the Administrator Console databases (`DrWebAdmin.nsf`).

12.3. Why is the Anti-spam component not working?

If Dr.Web does not detect spam or the Anti-spam settings are unavailable, it is likely that your license key file does not support scanning for spam (see Licensing Parameters). In order to check this, using a text editor open the license key file (`C:\Program Files\DrWeb for Lotus Domino\drweb32.key`) and find the following string: `LotusSpamFilter=No`.

If the parameter is `LotusSpamFilter=Yes`, your key file does support the Anti-spam component. In this case contact Doctor Web technical support.

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

If Dr.Web service databases (`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 the following error message appears in the Lotus Domino server console window every 5 minutes:

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

The Post-Installation Setup section specifies what you need to do to sign the databases.

12.5. How to disable virus-detection features?

To disable virus detection without uninstalling Dr.Web, disable loading of the Monitor and Scanner anti-virus components.

To disable component loading

1. Open the `notes.ini` file of the Lotus Domino server where anti-virus application 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 component loading

1. Open the `notes.ini` file of the Lotus Domino server where anti-virus application 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.

12.6. 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,
- cldbdir.nsf,
- namagent.nsf,
- reports.nsf,
- schema.nsf,
- activity.nsf,
- AgentRunner.nsf,
- busytime.nsf,
- certsrv.nsf,
- dba4.nsf,
- doladmin.nsf,
- lndfr.nsf,
- statrep.nsf.

12.7. How to configure the plug-in via a web interface?

You can configure Dr.Web settings in a web browser via the Lotus Domino HTTP server.

To launch the 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 http://domino.server/drweb/DrWebAdmin.nsf.
4. Enter the name and *Internet password* of the administrator account specified in DrWeb Admin group.

12.8. Which files are updated by the Updater?

The Updater component of Dr.Web downloads and updates the following components:

- virus databases (`*.vdb`),
- Anti-spam engine (`vrcpp.dll`),
- scan engine (`drweb32.dll`),
- the Updater itself (`drwebupw.exe`).

The following components are 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`).

12.9. What replication types are there?

Two main 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 is installed on both servers which take part in the replication process, virus detection and document curing is carried out without any problems. However, if only one of the servers is protected, keep in mind the following aspects of the plug-in operation:

Action	Task which performs replication and virus detection	Comments
A protected server performs a PUSH-replication to an unprotected server	replica	An infected document on the protected server will be cured during replication, that is, the unprotected server will receive a cured document. However, the document

Action	Task which performs replication and virus detection	Comments
		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.

13. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

1. Download and review the latest manuals and guides at https://download.drweb.com/doc/.
2. See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
3. Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

1. Fill out a web form in the appropriate section at https://support.drweb.com/.
2. Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.