



Dr.WEB®

Enterprise Security Suite

Defend what you create

Appendices

© Doctor Web, 2015. 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!, Dr.Web 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 Enterprise Security Suite
Version 10.0
Appendices to Administrator Manual
23.11.2015**

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

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

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

Doctor Web

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

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

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

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



Table of Contents

Chapter 1: Welcome to Dr.Web® Enterprise Security Suite	7
Introduction	7
Conventions and Abbreviations	8
Chapter 2: Appendices	9
Appendix A. The Complete List of Supported OS Versions	9
Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver	14
B1. Setting Up the ODBC driver	15
B2. Setting Up the Database Driver for Oracle	17
B3. Using the PostgreSQL DBMS	19
Appendix C. Procedures for Authentication of Administrators	21
C1. Active Directory Authentication	21
C2. LDAP Authentication	22
C3. Permissions Inheriting	22
C4. Depended Permissions Sections	24
Appendix D. Notification System Settings	29
D1. Predefined Notifications Description	29
D2. The Description of the Notification System Parameters	32
D3. The Parameters of the Notification System Templates	34
Appendix E. The Specification of Network Addresses	40
E1. The General Format of Address	40
E2. The Addresses of Dr.Web Server	41
E3. The Addresses of Dr.Web Agent/ Installer	42
Appendix F. Administration of the Repository	43
F1. General configuration files	43
F2. Products configuration files	45
Appendix G. Configuration Files	49
G1. Dr.Web Server Configuration File	49
G2. Dr.Web Security Control Center Configuration File	62
G3. Download.conf Configuration File	66
G4. Proxy Server Configuration File	67
Appendix H. Command Line Parameters of the Programs Included in Dr.Web Enterprise Security Suite	71
H1. Introduction	71



H2. Network Installer	71
H3. Dr.Web Agent	74
H4. Dr.Web Server	75
H5. Administrating Utility of the Embedded Database	82
H6. Utility of Generation of Key Pairs and Digital Signatures	83
H7. Administration of Dr.Web Server Version for UNIX® OS with the kill Instruction	83
H8. Dr.Web Scanner for Windows®	84
H9. Proxy Server	84
H10. Dr.Web Server Remote Diagnostics Utility	85
H11. Dr.Web Server Installer for UNIX® System-Based OS	90
Appendix I. Environment Variables Exported by Dr.Web Server	92
Appendix J. Regular Expressions Used in Dr.Web Enterprise Security Suite	93
J1. Options Used in PCRE Regular Expressions	93
J2. Peculiarities of PCRE Regular Expressions	94
Appendix K. Log Files Format	96
Appendix L. Integration of Web API and Dr.Web Enterprise Security Suite	98
Appendix M. Licenses	99
M1. Boost	100
M2. Curl	100
M3. Libradius	101
M4. Net-snmp	101
M5. OpenLDAP	106
M6. OpenSSL	107
M7. Oracle Instant Client	109
M8. PCRE	113
M9. Wtl	114
M10. Zlib	118
M11. MIT License	118
M12. GNU General Public License	119
M13. GNU Lesser General Public License	127
M14. Mozilla Public License	129
M15. GCC runtime libraries	135
Chapter 3: Frequently Asked Questions	137
Moving Dr.Web Server to Another Computer (under Windows® OS)	137
Connecting Dr.Web Agent to Other Dr.Web Server	139
Changing the Type of the DBMS for Dr.Web Enterprise Security Suite	141



Restoring the Database of Dr.Web Enterprise Security Suite	144
Restoring Dr.Web Server from Data Backup	148
Upgrading Dr.Web Agents on the LAN servers	150
Restoring the Password of Dr.Web Enterprise Security Suite Administrator	151
Using DFS During Installation of the Agent via the Active Directory	152
Chapter 4: Remote Installation Trouble Shooting	153
Index	155



Chapter 1: Welcome to Dr.Web® Enterprise Security Suite

Introduction

Documentation of **Dr.Web® Enterprise Security Suite** anti-virus network administrator is intended to introduce general features and provide detailed information on the organization of the complex anti-virus protection of corporate computers using **Dr.Web® Enterprise Security Suite**.

Documentation of **Dr.Web® Enterprise Security Suite** anti-virus network administrator contains the following parts:

1. **Installation Manual** (the **drweb-esuite-10-install-manual-en.pdf** file)
2. **Administrator Manual** (the **drweb-esuite-10-admin-manual-en.pdf** file)
3. **Appendices** (the **drweb-esuite-10-appendices-en.pdf** file)

Appendices provide technical information, describes the configuration parameters of the **Anti-virus** modules and explains the syntax and values of instructions used for operation with them.



Administrator documentation contains cross-references between three mentioned documents. If you download these documents to the local computer, cross-references work only if documents are located in the same folder and have their initial names.

Administrator documentation does not include the description of **Dr.Web** anti-virus packages for protected computers. For relevant information, please consult **User Manuals** of **Dr.Web** anti-virus solution for corresponding operating system.

Before reading these document make sure you have the latest version of the Manuals. The Manuals are constantly updated and the current version can always be found at the official web site of **Doctor Web** at <http://download.drweb.com/esuite/>.





Conventions and Abbreviations

Conventions

The [following](#) conventions are used in the Manual.

Table 1-1. Conventions

Symbol	Comment
 Note, that	Marks important notes or instructions.
 Warning	Warns about possible errors.
Dr.Web Scanner	Names of Dr.Web products and components.
<i>Anti-virus network</i>	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
Cancel	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, input to the command line and application output.
Appendix A	Cross-references or Internal Hyperlinks to web pages.

Abbreviations

The following abbreviations will be used in the Manual without further interpretation:

- ◆ ACL – Access Control List,
- ◆ CDN – Content Delivery Anti-virus network,
- ◆ DB, DBMS – Database, Database Management System,
- ◆ DFS – Distributed File System,
- ◆ DNS – Domain Name System,
- ◆ **Dr.Web GUS – Dr.Web Global Update System,**
- ◆ EBNF – Extended Backus-Naur Form,
- ◆ GUI – Graphical User Interface, a GUI version of a program – a version using a GUI,
- ◆ LAN – Local Area Network,
- ◆ MTU – Maximum Transmission Unit,
- ◆ NAP – Network Access Protection,
- ◆ OS – operating system,
- ◆ PC – personal computer,
- ◆ TTL – Time To Live,
- ◆ UDS – UNIX domain socket.



Chapter 2: Appendices

Appendix A. The Complete List of Supported OS Versions

For Dr.Web Server

UNIX system-based OS

ALT Linux School Server 5.0
ALT Linux School Server 5.0 x86_64
ALT Linux School 6.0
ALT Linux School 6.0 x86_64
ALT Linux SPT 6.0 certified by FSTEC
ALT Linux SPT 6.0 certified by FSTEC x86_64
Debian/GNU Linux 6.0 Squeeze
Debian/GNU Linux 6.0 Squeeze x86_64
Debian/GNU Linux 7.0 Wheezy
Debian/GNU Linux 7.0 Wheezy x86_64
Debian/GNU Linux 8.0 Jessie
Debian/GNU Linux 8.0 Jessie x86_64
FreeBSD 8.1
FreeBSD 8.1 amd64
FreeBSD 8.2
FreeBSD 8.2 amd64
FreeBSD 8.3
FreeBSD 8.3 amd64
FreeBSD 8.4
FreeBSD 8.4 amd64
FreeBSD 9.0
FreeBSD 9.0 amd64
FreeBSD 9.1
FreeBSD 9.1 amd64
FreeBSD 9.2
FreeBSD 9.2 amd64
FreeBSD 10.0
FreeBSD 10.0 amd64
FreeBSD 10.1
FreeBSD 10.1 amd64
openSUSE Linux 11.4
openSUSE Linux 11.4 x86_64
openSUSE Linux 12
openSUSE Linux 12 x86_64
openSUSE Linux 13
openSUSE Linux 13 x86_64
openSUSE Linux 13.2



openSUSE Linux 13.2 x86_64
RedHat Enterprise Linux 5
RedHat Enterprise Linux 5 x86_64
RedHat Enterprise Linux 5.3
RedHat Enterprise Linux 5.3 x86_64
RedHat Enterprise Linux 6
RedHat Enterprise Linux 6 x86_64
RedHat Enterprise Linux 6.1
RedHat Enterprise Linux 6.1 x86_64
RedHat Enterprise Linux 7
RedHat Enterprise Linux 7 x86_64
RedHat Fedora 16
RedHat Fedora 16 x86_64
RedHat Fedora 17
RedHat Fedora 17 x86_64
RedHat Fedora 18
RedHat Fedora 18 x86_64
RedHat Fedora 19
RedHat Fedora 19 x86_64
RedHat Fedora 20
RedHat Fedora 20 x86_64
RedHat Fedora 21
RedHat Fedora 21 x86_64
RedHat Fedora 22
RedHat Fedora 22 x86_64
SUSE Linux Enterprise Server 10
SUSE Linux Enterprise Server 10 x86_64
SUSE Linux Enterprise Server 11
SUSE Linux Enterprise Server 11 x86_64
SUSE Linux Enterprise Server 12
SUSE Linux Enterprise Server 12 x86_64
Oracle Solaris 10 x86
Oracle Solaris 10 Sparc 32bit
Oracle Solaris 10 Sparc 64bit
Oracle Solaris 11 x86
Oracle Solaris 11 Sparc 32bit
Oracle Solaris 11 Sparc 64bit
Ubuntu 10.04
Ubuntu 10.04 x86_64
Ubuntu 12.04
Ubuntu 12.04 x86_64
Ubuntu 14.04
Ubuntu 14.04 x86_64
Ubuntu 15.04
Ubuntu 15.04 x86_64
Linux glibc2.13
Linux glibc2.13 x86_64



Linux glibc2.14
Linux glibc2.14 x86_64
Linux glibc2.15
Linux glibc2.15 x86_64
Linux glibc2.16
Linux glibc2.16 x86_64
Linux glibc2.17
Linux glibc2.17 x86_64
Linux glibc2.18
Linux glibc2.18 x86_64
Linux glibc2.19
Linux glibc2.19 x86_64
Linux glibc2.20
Linux glibc2.20 x86_64
Linux glibc2.21
Linux glibc2.21 x86_64
Astralinux 1.2 x86_64
Astralinux 1.3 x86_64
MCBC 3.0
MCBC 5.0 x86_64

Windows OS

- *32 bit:*

Windows XP Professional with SP3
Windows Server 2003 with SP2
Windows Vista
Windows Server 2008
Windows 7
Windows 8
Windows 8.1
Windows 10

- *64 bit:*

Windows Vista
Windows Server 2008
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows Server 2012 R2
Windows 8
Windows 8.1
Windows 10



For Dr.Web Agent and Anti-Virus Package

UNIX system-based OS

Linux glibc 2.13 and later for Intel x86/amd64 platforms on base of 2.6.37 core and later



For 64-bit versions of operating systems, support of 32-bit applications execution must be enabled.

The product was tested on the following **Linux** distributions (32-bit and 64-bit):

Linux distribution name	Versions	Required additional libraries for 64-bit OS version
Debian	7	libc6-i386
Fedora	20	glibc.i686
Mint	16, 17	libc6-i386
Ubuntu	12.04 LTS, 13.04, 13.10, 14.04, 14.10	libc6-i386
CentOS	5.10, 6.5, 7 (64-bit only)	glibc.i686
Red Hat Enterprise Linux	5.10, 6.5, 7 (64-bit only)	glibc.i686

Other **Linux** distributions that meet the above-mentioned requirements have not been tested for compatibility with **Anti-virus** but may be supported. If a compatibility issue occurs, contact technical support on the official website at <http://support.drweb.com/request/>.



If components of version **6** are connected to **Dr.Web Enterprise Security Suite**, please refer the documentation of the corresponding component to get information on the system requirements.

Windows OS

- 32 bit:

Windows XP Professional with SP2 and later

Windows Server 2003 with SP2

Windows Vista

Windows Server 2008

Windows 7

Windows 8

Windows 8.1

Windows 10

- 64 bit:

Windows Vista with SP2 and later

Windows Server 2008 with SP2

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows Server 2012 R2



Windows 8
Windows 8.1
Windows 10



For installation of **Dr.Web Agents** on stations operating under Windows Vista OS or Windows Server 2008 OS, it is recommended to install the SP2 updates for the corresponding operating system. Otherwise, errors caused by the functioning peculiarities of the operating system with an anti-virus software can be occurred.

Remote installation of **Dr.Web Agents** is not available on workstations under Windows OS of Starter and Home editions.

Novell NetWare OS

Novell NetWare 4.11 SP9
Novell NetWare 4.2
Novell NetWare 5.1
Novell NetWare 6.0
Novell NetWare 6.5

OS X

OS 10.6.6 (Snow Leopard)
OS 10.6.7 (Snow Leopard)
OS 10.6.8 (Snow Leopard)
OS 10.6.6 Server (Snow Leopard Server)
OS 10.6.7 Server (Snow Leopard Server)
OS 10.6.8 Server (Snow Leopard Server)
OS 10.7 (Lion)
OS 10.7 Server (Lion Server)
OS 10.8 (Mountain Lion)
OS 10.8 (Mountain Lion Server)
OS 10.9 (Mavericks)
OS 10.9 Server (Mavericks Server)

Android OS

Android 4.0
Android 4.1
Android 4.2
Android 4.3
Android 4.4
Android 5.0
Android 5.1.



Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver



You can get the structure of **Dr.Web Server** DB via the `init.sql` script, located in the `etc` subfolder of **Dr.Web Server** installation folder.

As a database for **Dr.Web Server** you can use the following variants:

- ◆ embedded DBMS;
- ◆ external DBMS.

Embedded DBMS

When setting access to DBMS for storage and processing of data, use the parameters described in the table **B-1** for embedded DBMS.

Table B-1. Embedded DBMS (IntDB) parameters

Name	Default value	Description
DBFILE	database.sqlite	Path to the database file
CACHESIZE	2000	Database cache size in pages
SYNCHRONOUS	FULL	Mode of synchronous logging of changes in the database to the disk: <ul style="list-style-type: none">• FULL – fully synchronous logging to the disk,• NORMAL – synchronous logging of critical data,• OFF – asynchronous logging.

The following DBMS are provided as embedded:

- ◆ IntDB - modified version of SQLite 2.
- ◆ SQLite3 - DBMS that is supported by the **Server** starting from version **10**. SQLite3 has several advantages over the previous SQLite2 version, particularly:
 - more compact format for database file;
 - data bit capacity is increased: 64-bit rows identifiers are supported, text data is supported in both UTF-8 and UTF-16 formats;
 - BLOB data type is supported;
 - concurrent requests to the database are improved;
 - etc.



It is recommended to use SQLite3 if you select embedded database.

External DBMS

The following database management systems may be used to arrange the external database for **Dr.Web Server**:

- ◆ Oracle. The settings are given in Appendix B2. [Setting Up the Database Driver for Oracle](#).
- ◆ PostgreSQL. The settings necessary for PostgreSQL are given in Appendix B4. [Using the PostgreSQL DBMS](#).



- ◆ Microsoft SQL Server/Microsoft SQL Server Express. To access these DBMS, an ODBC driver may be used (setting up the parameters of the ODBC driver for Windows is given in Appendix B1. [Setting Up the ODBC Driver](#)).



With Microsoft SQL Server 2005 it is necessary to use the ODBC driver supplied with this DBMS.

Using of Microsoft SQL Server 2005 (SP4) and later is supported.

It is strongly recommended to install latest service packs for used DB server.

Microsoft SQL Server Express DB is not recommended for anti-virus network with a large number of stations (from 100 and more).

If the Microsoft SQL Server is used as an external DB for the **Server** under UNIX system-based OS, the proper operation via the ODBC with FreeTDS is not guaranteed.

If the Microsoft SQL Server is used as an external DB, it is necessary to use collation corresponding to **Dr.Web Server** language.

Comparison Characteristics



An embedded DB can be used, if at most 200-300 stations are connected to the **Server**. If the hardware configuration of the computer with **Dr.Web Server** and the load level of other executing tasks are permissible, up to 1000 stations can be connected.

Otherwise, you must use an external DB.

If you use an external DB and more than 10 000 stations are connected to the **Server**, it is recommended to perform the following minimal requirements:

- ◆ 3 GHz processor CPU,
- ◆ RAM at least 4 GB for **Dr.Web Server** and at least 8 GB for the DB server,
- ◆ UNIX system-based OS.

When choosing between an embedded and external database, take into account the following peculiar parameters of DMBS:

- ◆ In large anti-virus networks (of over 200-300 stations), it is recommended to use an external DB, which is more fault-resistant than embedded DBs.
- ◆ The embedded DBMS is considerably faster than the external analogs and is recommended mainly for the typical use of databases.
- ◆ You may use an external database in case it will be necessary to work through a DBMS and access the DB directly. To facilitate access, standard APIs may be used, such as OLE DB, ADO.NET or ODBC.

B1. Setting Up the ODBC driver

When setting access to DBMS for storage and processing of data, use the parameters described in the table **B-2** for external DBMS.

Table B-2. Parameters for ODBC connection

Name	Default value	Description
DSN	Drwcs	Data set name
USER	Drwcs	User name
PASS	Drwcs	Password
TRANSACTION	DEFAULT	Possible values of the TRANSACTION parameter:



Name	Default value	Description
		<ul style="list-style-type: none">• SERIALIZABLE• READ_UNCOMMITTED• READ_COMMITTED• REPEATABLE_READ• DEFAULT <p>The <code>DEFAULT</code> value means "use default of the SQL server". More information on transactions isolation see in documentation on corresponding DBMS.</p>



To exclude encoding problems, you must disable the following parameters of ODBC-driver:

- ◆ **Use regional settings when outputting currency, numbers, dates and times** - may cause errors during numerical parameters formatting.
- ◆ **Perform translation for character** - may cause illegal characters displaying in **Dr.Web Security Control Center** for parameters, which are came from the DB. This parameter sets symbols displaying dependence on the language parameter for programs, which do not use the Unicode.

The database is initially created on the SQL server with the above mentioned parameters.

It is also necessary to set the ODBC driver parameters on the computer where **Dr.Web Server** is installed.



Information on ODBC driver setup under UNIX system-based OS you can find at <http://www.unixodbc.org/> in the **Manuals** section.

ODBC Driver Setup for Windows OS

To configure ODBC driver parameters:

1. In Windows OS **Control Panel**, select **Administrative tools**; in the opened window double-click **Data Sources (ODBC)**. The **ODBC Data Source Administrator** window will be opened. Go to the **System DSN** tab.
2. Click **Add**. A window for selecting a driver will be opened.
3. Select the item of the corresponding ODBC-driver for this DB in the list and click **Finish**. The first window for setting access to the DB server will be opened.



If an external DBMS is used, it is necessary to install the latest version of the ODBC driver delivered with this DBMS. It is strongly recommended not to use the ODBC driver supplied with Windows OS. Except databases, supplied by Microsoft without ODBC-driver.

4. Specify access parameters to the data source, the same as parameters in the settings of **Dr.Web Server**. If the DB server is not installed on the same computer as **Dr.Web Server**, in the **Server** field, specify IP address or name of the DB server. Click **Next**.
5. Select the **With SQL Server authentication** option and specify necessary user credentials to access the DB. Click **Next**.
6. In the **Change the default database to** drop-down list, select the database which is used by **Dr.Web Server**. At this, the **Server** database name must be obligatory specified, but not the **Default** value.



Make sure that the following flags are set: **Use ANSI quoted identifiers** and the **Use ANSI nulls, paddings and warnings**. Click **Next**.



If ODBC driver settings allow you to change the language of SQL server system messages, select **English**.

7. When you complete the configuration, click **Finish**. A window with the summary of the specified parameters will be opened.
8. To test the specified settings, click **Test Data Source**. After notification of a successful test, click **OK**.

B2. Setting Up the Database Driver for Oracle

General Description

The Oracle Database (or Oracle DBMS) is an object-relational DBMS. Oracle may be used as an external DB for **Dr.Web Enterprise Security Suite**.



The **Dr.Web Server** may use the Oracle DBMS as an external database on all platforms except FreeBSD (see [Installation and supported versions](#)).

To use the Oracle DBMS:

1. Install an instance of Oracle DB and set up the `AL32UTF8` encoding. Also you may use existence instance which is configured to use the `AL32UTF8` encoding.
2. Set up the database driver to use the respective external database. You can do this in [configuration file](#) or via **Dr.Web Security Control Center: Dr.Web Server configuration, Database** tab.



If you are going to use the Oracle DB as an external database via the ODBC connection, then during installation (upgrading) of the **Server**, in the installer settings, select the **Custom** option of the installation and in the next window disable the installation of embedded client for Oracle DBMS (in the **Database support - Oracle database driver** section).

Otherwise, interaction with the Oracle DB via ODBC will fail because of the libraries conflict.

Installation and Supported Versions

To use Oracle as an external DB, you must install the instance of the Oracle DB and set up `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`) encoding. This can be done in one of the following ways:

1. Using an Oracle installer (use an external mode of instance installation and configuration).
2. Using the `CREATE DATABASE SQL` command.

For more information on creating and configuring Oracle instances, see Oracle documentation.



In case of using a different encoding, national symbols may be displayed incorrectly.



A client to access the database (Oracle Instant Client) is included in the installation package of **Dr.Web Enterprise Security Suite**.

Platforms supported by the Oracle DBMS are listed on the web site of the vendor <http://www.oracle.com/technology/software/tech/oci/instantclient/index.html>.

Dr.Web Enterprise Security Suite supports the following versions of the DBMS: Oracle9i Database Release 2: 9.2.0.1 - 9.2.0.8 and higher.

Parameters

To adjust access to the Oracle DBMS, use the parameters described in Table B-3.

Table B-3. Parameters of the Oracle DBMS

Parameter	Description
drworacle	Driver name
User	Database user name (obligatory)
Password	User password (obligatory)
ConnectionString	Database connection string (obligatory)

The format of the connection string to the Oracle DBMS is as follows:

`//<host>:<port>/<service name>`

where:

- ◆ `<host>` - IP address or name of the Oracle server;
- ◆ `<port>` - port that the server is 'listening';
- ◆ `<service name>` - name of the DB to connect to.

For Example:

`//myserver111:1521/bjava21`

where:

- ◆ `myserver111` - name of the Oracle server.
- ◆ `1521` - port 'listening' to the server.
- ◆ `bjava21` - name of the DB to connect to.

Oracle DBMS Driver Configuration

If you deploy Oracle, it is necessary to change the definition and the settings of the database driver by one of the following ways:

- ◆ In the **Control Center: Administration** item in the main menu → **Dr.Web Server configuration** item in the control menu → **Database** tab → select in the **Database** drop-down list, the **Oracle** type, and set parameters according to the format listed below.
- ◆ In the [Server configuration file](#).



B3. Using the PostgreSQL DBMS

General Description

PostgreSQL is an object-relational DBMS distributed as a freeware unlike such commercial DBMS as Oracle Database, Microsoft SQL Server, etc. The PostgreSQL DBMS may be used to arrange an external DB for **Dr.Web Enterprise Security Suite** in large anti-virus networks.

To do this:

1. Install the PostgreSQL server.
2. Set up **Dr.Web Server** to use the respective external database. You can do this in [configuration file](#) or via **Dr.Web Security Control Center: Dr.Web Server configuration, Database** tab.



If you are going to use the PostgreSQL DB as an external database via the ODBC connection, then during installation (upgrading) of the **Server**, in the installer settings, select the **Custom** option of the installation and in the next window disable the installation of embedded client for PostgreSQL DBMS (in the **Database support - PostgreSQL database driver** section).

Otherwise, interaction with the PostgreSQL DB via ODBC will fail because of the libraries conflict.

To connect to the PostgreSQL DB you can use only trust authorization, password and MD5 (Kerberos, GSS and SSPI are not supported).

Installation and Supported Versions

Please download the latest available version of this free product (the **PostgreSQL** server and correspondent ODBC-driver), otherwise do not use the version earlier than **8.4**.

For more information about conversion to the external database see p. [Changing the Type of the DBMS for Dr.Web Enterprise Security Suite](#).

Parameters

When setting access to PostgreSQL, use parameters described in the table **B-4**.

Table B-4. PostgreSQL parameters

Name	Default value	Description
host	<UNIX domain socket>	PostgreSQL server host
port		PostgreSQL server port or name extension of the socket file
dbname	drwcs	Database name
user	drwcs	User name
password	drwcs	Password
options		Debug/trace options for sending to the Server
tty		File or tty to output at debug
requiressl		1 instructs to request a SSL connection; 0 does not instruct to make the request
temp_tablespaces		Name space for temporary tables



Name	Default value	Description
default_transaction_isolation		Transaction isolation mode (see PostgreSQL documentation)

More information can be found at <http://www.postgresql.org/docs/manuals/>.

Dr.Web Server and PostgreSQL DB Interaction via the UDS

If **Dr.Web Server** and the PostgreSQL DB are installed on the same computer, their interaction can be set via the UDS (UNIX domain socket).

To set interaction via the UDS:

1. In the `postgresql.conf` PostgreSQL configuration file, specify the following directory for the UDS:

```
unix_socket_directory = '/var/run/postgresql'
```

2. Restart the PostgreSQL.



Appendix C. Procedures for Authentication of Administrators



General information on authentication of administrators at **Dr.Web Server** is described in **Administrator Manual**, p. [Authentication of Administrators](#).

C1. Active Directory Authentication

Only enabling of using authentication method and the order in authenticators list are configured: in the `<enabled/>` and `<order/>` tags of the `auth-ads.xml` configuration file.

Operation principle:

1. Administrator specifies username and password in one of the following formats:
 - ◆ username,
 - ◆ domain\username,
 - ◆ username@domain,
 - ◆ user's LDAP DN.
2. Server registers with these name and password at the default domain controller (or at the domain controller which specified in the username).
3. If registration failed, transition to the next authentication mechanism is performed.
4. LDAP DN of registered user is determined.
5. For the object with determined DN, the `DrWebAdmin` attribute is read. If it has `FALSE` value, authentication is admitted failed and transition to the next authentication mechanism is performed.
6. If any of attributes are not defined at this stage, they are searched in groups to which the user is included to. For each group, its parental groups are checked (search strategy - inward).



If any error occurs, transition to the next authentication mechanism is performed.

The `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxxxxx-windows-nt-xYY.exe` utility (is included to the **Server** distribution kit) creates in Active Directory the `DrWebEnterpriseUser` new object class and defines new attributes for this class.

Attributes have the following OID in the **Enterprise** space:

```
#define DrWeb_enterprise_OID      "1.3.6.1.4.1"           //
iso.org.dod.internet.private.enterprise
#define DrWeb_DrWeb_OID          DrWeb_enterprise_OID      ".29690"          // DrWeb
#define DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID         ".1"             // EnterpriseSuite
#define DrWeb_Alerts_OID         DrWeb_EnterpriseSuite_OID ".1"             // Alerts
#define DrWeb_Vars_OID           DrWeb_EnterpriseSuite_OID ".2"             // Vars
#define DrWeb_AdminAttrs_OID     DrWeb_EnterpriseSuite_OID ".3"             // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSuite.AdminAttrs.Admin)

#define DrWeb_Admin_OID          DrWeb_AdminAttrs_OID     ".1"             // R/W admin
#define DrWeb_AdminReadOnly_OID  DrWeb_AdminAttrs_OID     ".2"             // R/O admin
#define DrWeb_AdminGroupOnly_OID DrWeb_AdminAttrs_OID     ".3"             // Group admin
#define DrWeb_AdminGroup_OID     DrWeb_AdminAttrs_OID     ".4"             // Admin's group
#define DrWeb_Admin_AttrName     "DrWebAdmin"
#define DrWeb_AdminReadOnly_AttrName "DrWebAdminReadOnly"
#define DrWeb_AdminGroupOnly_AttrName "DrWebAdminGroupOnly"
#define DrWeb_AdminGroup_AttrName "DrWebAdminGroup"
```



Editing settings of Active Directory users is implemented manually at the Active Directory server (see **Administrator Manual**, p. [Authentication of Administrators](#)).

Assigning permissions to administrators performs according to the general principle of inheriting in the hierarchical structure of groups in which administrator is included.

C2. LDAP Authentication

Settings are stored in the `auth-ldap.xml` configuration file.

General tags of the configuration file:

- ◆ `<enabled/>` and `<order/>` - similar to the Active Directory.
- ◆ `<server/>` specifies the LDAP server address.
- ◆ `<user-dn/>` defines rules for translation of name to the DN (Distinguished Name) using DOS-like masks.

In the `<user-dn/>` tag, the following wildcard characters are allowed:

- `*` replaces sequence of any characters, except `.`, `,`, `=`, `@`, `\` and spaces;
- `#` replaces sequence of any characters.
- ◆ `<user-dn-expr/>` defines rules for translation of name to the DN using regular expressions.

For example, the same rule in different variants:

```
<user-dn user="*@example.com" dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr user="(.*).*@example.com" dn="CN=\1,DC=example,DC=com"/>
```

`\1 .. \9` defined the substitution place for values of the `*` symbol or expression in brackets at the template.

According to this principle, if the user name is specified as `login@example.com`, after translation you will get DN: `"CN=login,DC=example,DC=com"`.

- ◆ `<user-dn-extension-enabled/>` allows the `ldap-user-dn-translate.ds` (from the `extensions` folder) Lua-script execution for translation usernames to DN. This script runs after attempts of using the `user-dn`, `user-dn-expr` rules, if appropriate rule is not found. Script has one parameter - specified username. Script returns the string that contains DN or nothing. If appropriate rule is not found and script is disabled or returns nothing, specified username is used as it is.
- ◆ Attributes of LDAP object for DN determined as a result of translation and their possible values can be defined by tags (default values are presented):

```
<!-- DrWebAdmin attribute equivalent (OID 1.3.6.1.4.1.29690.1.3.1) -->
<admin-attribute-name value="DrWebAdmin" true-value="^TRUE$" false-value="^FALSE$"/>
```

As a values of `true-value/false-value` parameters, regular expressions are specified.

- ◆ If undefined values of administrators attributes are present, and the `<group-reference-attribute-name value="memberOf"/>` tag is set in the configuration file, the value of the `memberOf` attribute is considered as the list of DN groups, to which this administrator is included, and the search of needed attributes is performed in this groups as for the Active Directory.

C3. Permissions Inheriting

The table below contains calculated result rights of an object (administrator or administrative group) depending on inheritance and parental groups rights.



Table C-1. Table of permissions inheriting

№	Previous right			Current group			Result right		
	Inheritance	Group is set	Right is set	Inheritance	Group is set	Right is set	Inheritance	Group is set	Right is set
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	1	0	0	1
2	0	0	0	0	1	0	0	0	0
3	0	0	0	0	1	1	0	1	1
4	0	0	0	1	0	0	0	0	0
5	0	0	0	1	0	1	1	0	1
6	0	0	0	1	1	0	0	0	0
7	0	0	0	1	1	1	1	1	1
8	0	0	1	0	0	0	0	0	1
9	0	0	1	0	0	1	0	0	1
10	0	0	1	0	1	0	0	0	1
11	0	0	1	0	1	1	0	0	1
12	0	0	1	1	0	0	0	0	1
13	0	0	1	1	0	1	1	0	1
14	0	0	1	1	1	0	0	0	1
15	0	0	1	1	1	1	1	1	1
16	0	1	0	0	0	0	0	0	0
17	0	1	0	0	0	1	0	0	1
18	0	1	0	0	1	0	0	0	0
19	0	1	0	0	1	1	0	1	1
20	0	1	0	1	0	0	0	0	0
21	0	1	0	1	0	1	1	0	1
22	0	1	0	1	1	0	0	0	0
23	0	1	0	1	1	1	1	1	1
24	0	1	1	0	0	0	0	1	1
25	0	1	1	0	0	1	0	0	1
26	0	1	1	0	1	0	0	1	1
27	0	1	1	0	1	1	0	1	1
28	0	1	1	1	0	0	0	1	1
29	0	1	1	1	0	1	0	1	1
30	0	1	1	1	1	0	0	1	1
31	0	1	1	1	1	1	1	1	1
32	1	0	0	0	0	0	0	0	0
33	1	0	0	0	0	1	0	0	1
34	1	0	0	0	1	0	0	0	0
35	1	0	0	0	1	1	0	1	1
36	1	0	0	1	0	0	0	0	0
37	1	0	0	1	0	1	1	0	1
38	1	0	0	1	1	0	0	0	0



№	Previous right			Current group			Result right		
	Inheritance	Group is set	Right is set	Inheritance	Group is set	Right is set	Inheritance	Group is set	Right is set
39	1	0	0	1	1	1	1	1	1
40	1	0	1	0	0	0	1	0	1
41	1	0	1	0	0	1	0	0	1
42	1	0	1	0	1	0	1	0	1
43	1	0	1	0	1	1	0	1	1
44	1	0	1	1	0	0	1	0	1
45	1	0	1	1	0	1	1	0	1
46	1	0	1	1	1	0	1	0	1
47	1	0	1	1	1	1	1	1	1
48	1	1	0	0	0	0	0	0	0
49	1	1	0	0	0	1	0	0	1
50	1	1	0	0	1	0	0	0	0
51	1	1	0	0	1	1	0	1	1
52	1	1	0	1	0	0	0	0	0
53	1	1	0	1	0	1	1	0	1
54	1	1	0	1	1	0	0	0	0
55	1	1	0	1	1	1	1	1	1
56	1	1	1	0	0	0	1	1	1
57	1	1	1	0	0	1	0	0	1
58	1	1	1	0	1	0	1	1	1
59	1	1	1	0	1	1	0	1	1
60	1	1	1	1	0	0	1	1	1
61	1	1	1	1	0	1	1	1	1
62	1	1	1	1	1	0	1	1	1
63	1	1	1	1	1	1	1	1	1

C4. Depended Permissions Sections

Table C-2. The list of administrative rights and their features

№	Permission	Description	Control Center section
1*	View groups of stations properties	The list of user groups which administrator sees in the anti-virus network. All system groups are also displayed in the anti-virus network tree, but only stations from the specified group list are available inside.	Anti-virus Network Anti-virus Network > General > Properties
2*	Edit groups of stations properties	The list of user groups, properties of which administrator can edit. Must contain groups from the list of permission 1.	



Nº	Permission	Description	Control Center section
3	View groups of stations configuration	The list of user groups, configuration of which is available to view by administrator. Also, administrator is permitted to view configuration of stations, for which the groups from the list are primary. Must contain groups from the list of permission 1.	Anti-virus Network Anti-virus Network > General > Running components Anti-virus Network > General > Quarantine
4	Edit groups of stations configuration	Same as permission 3, but editing is permitted. Must contain groups from the list of permission 3.	Pages from the Configuration section
5	View stations properties	The list of user groups that are primary for stations properties of which administrator is permitted to view. Must contain groups from the list of permission 1.	Anti-virus Network Anti-virus Network > General > Properties
6	Edit stations properties	Including ACL, blocking, access, etc. Same as permission 5, but editing is permitted. Must contain groups from the list of permission 5.	
8*	Move stations into groups and remove stations from groups	The list of user groups. Must contain groups from the list of permission 1.	
9	Delete stations	The list of user groups that are primary for stations which administrator can delete. Must contain groups from the list of permission 1.	
10	Remote Agent installation and deinstallation	The list of user groups, for stations of which administrator is permitted to run remote installation of Agents with selected ID. These groups must be a primary for installing stations. Must contain groups from the list of permission 1. Menu item is not displayed if there are forbidden objects. Network installation is available from the /esuite/network/index.ds only in if 16 permission is allowed.	Anti-virus Network
11	Merge stations	The list of user groups stations of which can be merged. These groups must be a primary for stations. The icon to merge stations is available on the toolbar. Must contain groups from the list of permission 1.	
12*	View statistic tables	The list of user groups statistics of which can be viewed by administrator.	Anti-virus Network pages from the Statistics section



№	Permission	Description	Control Center section
		<p>The permission allows to create a task in the Server schedule to receive periodically reports. The list of user groups which administrator can be specify in the task is set (groups for stations of which the reports will be received). If Everyone is set, reports will be received for all groups from the list.</p> <p>Must contain groups from the list of permission 1.</p>	
23	Edit licensing	<p>The list of user groups for which administrator can add/change/remove a license key. These groups must be a primary for the stations.</p> <p>Must contain groups from the list of permission 1.</p>	Administration > Administration > License manager
35	Create tariff group (AV-Desk)	Create user tariff group.	Anti-virus Network
36	View tariff group (AV-Desk)	The list of user tariff groups which are available for administrator in the anti-virus network.	Anti-virus Network
37	Edit tariff group (AV-Desk)	Must contain groups from the list of permission 36.	Anti-virus Network > General > Properties
38	Delete tariff group (AV-Desk)		Anti-virus Network
25	Create administrators, administrative groups	The corresponding icon in the toolbar is hidden either.	
26	Edit administrators accounts	<p>Administrator from the Newbies group sees only a tree of administrators, the root node of which is a group of this administrator, i.e. sees administrators from the own group and its subgroups. Administrator from the Administrators group sees all other administrators not depending on their groups.</p> <p>Administrator can edit administrative accounts from the specified groups. At this, the corresponding icon in the toolbar become available.</p>	Administration > Configuration > Administrators
27	Delete administrators accounts	Same as permission 26.	
28	View properties and configuration of administrative groups	<p>Including administrators in groups and subgroups.</p> <p>Administrator is able to select only from the subgroup of the own parent group.</p>	
29	Edit properties and configuration of administrative groups	<p>Including administrators in groups and subgroups.</p> <p>Administrator can select only from a subgroup of own parental group.</p>	



Nº	Permission	Description	Control Center section
		If this permission is denied, even if permission 26 is allowed for this groups, administrator will not be able to disable inheritance or increase permissions to administrator in the group.	
7	Create stations	At station creation, only the list of groups with permission 8 is available (group to which stations are placed, must have the 8 permission). At station creation, one of available user groups must become primary.	Anti-virus Network
13	View audit	Audit is available for full-rights administrator and for objects with permission 4.	Administration > Statistics > Audit log
14	View reports (AV-Desk)	Whether AV-Desk reports are available. Report contains stations from the list groups of permission 1.	
15	Send reports (AV-Desk)	The list from permission 14.	
16	Run Network scanner	If the permission is denied, the network installation for the /suite/network/index.ds is not available.	Anti-virus Network Administration > Network scanner
17	Approve newbies	The groups list from permission 8 is available.	Anti-virus Network
18	View Server schedule	The Tasks execution log table viewing. If the 12 and 18 permissions are forbidden, the view of the Server schedule page is forbidden. If the 12 permission is allowed but the 18 is forbidden, when viewing statistics schedule is available. The task for sending reports for respective administrator is displayed depending on the presence of the 12 permission and Periodic report , notification even if the 18 permission is forbidden.	Administration > Configuration > Dr.Web Server Task Scheduler Administration > Statistics > Task execution log
19	Edit Server schedule		Administration > Configuration > Dr.Web Server Task Scheduler
20	View Server configuration and repository configuration		Administration > Configuration > Web server configuration Administration > Repository > Repository state Administration > Repository > Delayed updates Administration > Repository > General repository configuration Administration > Repository > Detailed repository configuration



Nº	Permission	Description	Control Center section
21	Edit Server configuration and repository configuration		Administration > Repository > Repository content Administration > Repository > Update log of repository
22	View license information		
23			
24	Edit notifications configuration		Administration > Notifications > Notifications configuration Administration > Notifications > Unsent notifications Administration > Notifications > Web console notifications
30	Operation via XML API		
31	View neighborhood connections		
32	Edit neighborhood connections		
33	Use additional features	Limits access to all subsections of Additional features section except the Utilities subsection which is always available.	Administration > Additional features
34	Update repository	Update Server repository from GUS .	The Update repository button in the Repository state section

* Permissions 1, 2, 8, 12 are defined for station by the list of groups into which it is included but not by a primary group of the station.

If a station is included into the group and for the group some of these permissions are granted, when administrator will have access to the functions corresponding to these permissions not depending on whether the group is primary for the station or not. At this, granting is in priority: if a station is included into both granted and denied groups, administrator will have access to the functions corresponding to the permissions of granted group.



Appendix D. Notification System Settings



Base information on configuration of administrative notifications is given in the **Administrator Manual**, p. [Setting Notifications](#).

D1. Predefined Notifications Description



Variables used at notification templates editing are described in the [Application D3](#).

Notification name	Notification sending reason	Additional information
Administrator		
Administrator authorization failed	Sent on error of administrator authorization in the Control Center . The reason of authorization failure is given in the notification text.	
Unknown administrator	Sent on attempt of authorization in the Control Center by administrator with unknown login.	
Installation		
Installation failed	Sent if an error occurred during the Agent installation on a station. The error reason is given in the notification text.	
Installation successful	Sent on succeeded Agent installation on a station.	
License limit		
Agent key has expired	Sent if the Agent key has already expired.	
Allowed number of licenses is exceeded	Sent if the number of requested licenses for donation to a neighbor Servers exceeds the number of licenses that are available in the license key.	
Allowed number of stations is exceeded	Sent if during connection of a station to the Server , it was detected that the number of stations in the group into which the connected station is included, reached the limitation in the license key assigned for this group.	
Licenses donation has expired	Sent if the period of licenses donation to neighbor Servers from the license key of this Server has expired.	The period of licenses donation to neighbor Servers is specified in the Administration > Dr.Web Server configuration > Licenses section.
Number of stations is close to allowed limit	Sent if the number of stations in the group is closing to the license limitation in the key assigned to this group.	The number of available licenses left in the key to send the notification is: less than three licenses or less than 5% from the total number of licenses in the key.



Notification name	Notification sending reason	Additional information
The number of stations in database is exceeded	Sent if during the Server startup, it was detected that the number of stations in a group already exceeded the number of licenses in the license key assigned to this group.	
Newbie		
Station rejected automatically	Sent if a new station requested a connection to the Server and has been rejected by the Server automatically.	The situation may occur if in the Administration > Dr.Web Server configuration > General section, for the Newbies registration mode option, the Always deny access value is set.
Station rejected by administrator	Sent if a new station requested a connection to the Server and has been rejected by administrator manually.	The situation may occur if in the Administration > Dr.Web Server configuration > General section, for the Newbies registration mode option, the Approve access manually value is set and an administrator selected the Anti-virus Network > Unapproved stations > Reject selected stations option for this station.
Waiting for approval	Sent if a new station requested a connection to the Server and administrator must approve or reject the station manually.	The situation may occur if in the Administration > Dr.Web Server configuration > General section, for the Newbies registration mode option, the Approve access manually value is set.
Other		
Epidemic	Sent if an epidemic detected in the anti-virus network. It means that during specified time period, it was detected more than specified number of threats in the network.	To be able to sent epidemic notifications, you must set the Track epidemic flag in the Administration > Dr.Web Server configuration > General section. Parameters on epidemic detection are set in the same section.
Log rotate error	Sent if an error occurred during rotation of the Server operation log. The reason of log rotation error is given in the notification text.	
Log write error	Sent when an error occurred during writing an information into the Server operation log. The reason of log write error is given in the notification text.	
Neighbor server has not connected for a long time	Sent according to the task in the Server schedule. Contains information that the neighbor Server has not connected to this Server for a long time. The date of last connection is given in the notification text.	The time period during which the neighbor Server should not get connected to send the notification, is set in the Neighbor server has not connected for a long time task of the Server schedule configured in the Administration > Dr.Web Server Task Schedule .
Periodic report	Sent after generation of periodic report according to the task in the Server schedule. Also, notification contains the path to download the report file.	The report is generated according to the Statistic reports task in the Server schedule configured in the Administration > Dr.Web Server Task Schedule .
Test message	Sent on clicking the Send test message button in the Administration > Notifications configuration section.	



Notification name	Notification sending reason	Additional information
Repository		
Low disk free space	Sent if on a disk where the Server <code>var</code> folder located, is running out of space.	Low disk space defined if it is less than 315 MB or less than 1000 nodes (for UNIX system based OS) left, if this values do not redefined by environment variables.
Product has been updated	Sent when repository update from the GUS successfully completed.	
Обновление продукта заморожено	Sent if the repository product was frozen by administrator. At this, update of this product from the GUS is not performed.	You can manage repository products including their frozen and unfrozen states in the Administration > Detailed repository configuration section.
Product is up-to-date	Sent if during repository updates check, it was detected that requested product is up-to-date. At this, update of this product from the GUS is not required.	
Product update failed	Sent if during update of a repository product from the GUS , an error has occurred. The name of the product and the reason of update error are given in the notification text.	
Repository update started	Sent if during repository updates check, it was detected that for requested products an update required. At this, the update from the GUS is launched.	
Station		
Access automatically provided to the station	Sent if a new station requested a connection to the Server and has been approved by the Server automatically.	The situation may occur if in the Administration > Dr.Web Server configuration > General section, for the Newbies registration mode option, the Approve access automatically value is set.
Cannot create the station account	Sent if a new stations account cannot be created on the Server . Error details are given in the Server log file.	
Connection aborted	Sent on abnormal termination of a connection with a client (station, Agent installer, neighbor Server).	
Error during scanning	Sent if a notification received from a station reports an error during scanning.	
Infection detected	Sent if a notification received from a station reports the threats detection. Administrative notification also contains detailed information on detected threats.	
Scan statistics	Sent if a notification received from a station reports a scan completion. Administrative notification also contains brief scan statistic.	



Notification name	Notification sending reason	Additional information
Station approved	Sent if a new station requested a connection to the Server and has been approved by administrator manually.	The situation may occur if in the Administration > Dr.Web Server configuration > General section, for the Newbies registration mode option, the Approve access manually value is set and an administrator selected the Anti-virus Network > Unapproved stations > Approve selected stations and set a primary group option for this station.
Station authorization failed	Sent if a station provided incorrect credentials when trying to connect to the Server . Further actions that depend on a stations approval policy, are also given in the notification.	Stations approval policy is set in the Newbies registration mode option of the Administration > Dr.Web Server configuration > General section.
Station has not connected to the server for a long time	Sent according to the task in the Server schedule. Contains information that the station has not connected to this Server for a long time. The date of last connection is given in the notification text.	The time period during which the station should not get connected to send the notification, is set in the Station has not connected for a long time task of the Server schedule configured in the Administration > Dr.Web Server Task Schedule .
Station is already logged in	Send on attempt to connect to the Server by a station with identifier which matches the identifier of a station already connected to the Server .	
Station must be rebooted	Sent if a notification received from a station reports that the product has been updated and the station restart is required.	
Station update failed	Sent if a notification received from a station reports an error during update of anti-virus components from the Server .	
Unknown station	Sent if a new station requested a connection to the Server , but was not allowed to review for approval or rejection of the registration.	

D2. The Description of the Notification System Parameters

The system of alerts for events connected with the anti-virus network components operation, the following types of messages sent are used:

- email notifications,
- notifications via Windows Messenger,
- notifications via the Web Console,
- notifications via SNMP,
- notifications via the **Agent** protocol,
- Push notifications.

Depending on the notification sent method, the sets of parameters in the key -> value format are required. For each method, the following parameters are set:

**Table D-1. General parameters**

Parameter	Description	Default value	Obligatory
TO	The set of notification receivers divided with the sign		yes
ENABLED	Enable or disable notification send	true or false	yes
_TIME_TO_LIVE	The number of notification resend attempts in case of fail	10 attempts	no
_TRY_PERIOD	Period in seconds between notification resend attempts	5 min., (send not often than ones in 5 min.)	no

The tables with parameter lists for different notification send types are given below.

Table D-2. Email notifications

Parameter	Description	Default value
FROM	Address of the sender email	drwcsd@\${host name}
TO	Address of the receiver email	-
HOST	SMTP server address	127.0.0.1
PORT	SMTP server port number	<ul style="list-style-type: none">• 25, if the SSL parameter is no• 465, if the SSL parameter is yes
USER	SMTP server user	"" is specified, at least one authorization method must be enabled, otherwise the mail will not be sent).
PASS	password of SMTP server user	""
STARTTLS	use the STARTTLS encryption	yes
SSL	use the SSL encryption	no
AUTH-CRAM-MD5	use the CRAM-MD5 authentication	no
AUTH-PLAIN	use the PLAIN authentication	no
AUTH-LOGIN	use the LOGIN authentication	no
AUTH-NTLM	use the NTLM authentication	no
SSL-VERIFYCERT	Validate the server SSL certificate	no
DEBUG	Enable debug mode, e.g., to resolve the problem when authorization failed	-

Table D-3. Notifications via Windows Messenger (the drwwnetm driver), for Windows OS version only:

Parameter	Description	Default value
TO	Computer network name	-



Windows network message system functions only under Windows OS with Windows Messenger (Net Send) service support.

Windows Vista OS and later do not support Windows Messenger service.

**Table D-4. Notifications via Web console**

Parameter	Description	Default value
TO	UUID of administrators, to which this notification will be send	-
SHOW_PERIOD	Time to store the message in seconds starting from the moment of receiving	86400 seconds, i.e. one day.

Table D-5. Notifications via SNMP

Parameter	Description	Default value
TO	SNMP receiving entity, e.g., IP address	-
DOMAIN	Domain	<ul style="list-style-type: none">localhost for Windows OS,"" - for UNIX system-based OS.
COMMUNITY	SNMP community or the context	public
RETRIES	The number of notification resend attempts that the API performed	5 attempts
TIMEOUT	Time in seconds after which the API performs the notification resend attempt	5 seconds

Table D-6. Notifications via the Agent protocol

Parameter	Description	Default value
TO	UUID of receiving stations	-
SHOW_PERIOD	Time to store the message in seconds starting from the moment of receiving	86400 seconds, i.e. one day.

Table D-7. Push notifications

Parameter	Description	Default value
TO	Devices tokens which applications are get after registration on the vendor server, e.g. Apple	-
SERVER_URL	URL relay of the server, used to send notification to the vendor server	-

D3. The Parameters of the Notification System Templates

The text for messages (sent by e-mail or **Windows Messenger**) is generated by a **Server** component named the templates processor on the basis of the templates files.



Windows network message system functions only under Windows OS with Windows Messenger (Net Send) service support.

Windows Vista OS and later do not support Windows Messenger service.

A template file consists of text and variables enclosed in braces. When editing a template file, the variables listed below can be used.



The templates processor does not perform recursive substitutions.

The variables are written as follows:

- ◆ {<VAR>} – substitute the current value of the <VAR> variable.



- ◆ {<VAR>:<N>} – the first <N> characters of the <VAR> variable.
- ◆ {<VAR>:<first>:<N>} – the value of <N> characters of the <VAR> variable that go after the first <first> characters (beginning from the <first>+1 symbol), if the remainder is less, it is supplemented by spaces on the right.
- ◆ {<VAR>:<first>:-<N>} – the value of <N> characters of the <VAR> variable that go after the first <first> characters (beginning from the <first>+1 symbol), if the remainder is less, it is supplemented by spaces on the left.
- ◆ {<VAR>/<original1>/<replace1>[/<original2>/<replace2>]} – replace specified characters of <VAR> variable with given characters: <original1> characters are replaced with <replace1> characters, <original2> characters are replaced with <replace2> characters, etc.

There is no limitation for the number of substitution pairs.

Table D-8. Notation of variables

Variable	Value	Expression	Result
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17.456

Conventions

° - whitespace.

Environment Variables

To form messages texts you can use environment variables of the **Server** process (the **System** user).

Environment variables are available in the **Control Center** messages editor, in the **ENV** drop-down list. Please note: the variables must be specified with the `ENV.` prefix (the prefix ends with a dot).

System Variables

- ◆ `SYS.TIME` – current system time,
- ◆ `SYS.DATE` – current system date,
- ◆ `SYS.DATETIME` – current system date and time,
- ◆ `SYS.VERSION` – **Server** version,
- ◆ `SYS.BUILD` – **Server** build date,
- ◆ `SYS.PLATFORM` – **Server** platform,
- ◆ `SYS.PLATFORM.SHORT` – short variant of `SYS.PLATFORM`,
- ◆ `SYS.OS` – **Server** operating system name,
- ◆ `SYS.BRANCH` – system version (**Server** and **Agents**),
- ◆ `SYS.SERVER` – product name (**Dr.Web Server**).

Shared Variables of Messages, the Agent

- ◆ `GEN.LoginTime` – station login time,
- ◆ `GEN.StationAddress` – station address,
- ◆ `GEN.StationID` – station UUID,



- ◆ GEN.StationName – station name,
- ◆ GEN.StationPrimaryGroupName – name of the station primary group,
- ◆ GEN.StationPrimaryGroupID – ID of the station primary group.

Shared Variables of Messages, Server Updating Subsystem

- ◆ GEN.CurrentRevision — current version identifier,
- ◆ GEN.NextRevision — updated version identifier,
- ◆ GEN.Folder — product location folder,
- ◆ GEN.Product — product description.

Message Variables United According to Message Types (for the Agent)

Administrator_Authorization_Failed:

- ◆ MSG.Login – login,
- ◆ MSG.Address – **Dr.Web Security Control Center** network address,
- ◆ MSG.LoginErrorCode – numeric error code;

Approved_Newbie:

- ◆ MSG.AdminName – administrator name,
- ◆ MSG.AdminAddress – **Dr.Web Security Control Center** address;

AutoApproved_Newbie: no variables are available;

Awaiting_Approval: no variables are available;

Cannot_Add_Station:

- ◆ MSG.ID – station UUID;

Connection_Terminated_Abnormally:

- ◆ MSG.Reason – reason for the termination,
- ◆ MSG.Type – client type;

Epidemic

- ◆ MSG.Infected - number of detected viruses,
- ◆ MSG.Virus - virus type,
- ◆ MSG.Action - action performed;

Infection:

- ◆ MSG.Component – component name,
- ◆ MSG.RunBy – component is launched by this user,
- ◆ MSG.ServerTime – event receipt time (GMT),
- ◆ MSG.ObjectName – infected object name,
- ◆ MSG.ObjectOwner – infected object owner,
- ◆ MSG.InfectionType – infection type,
- ◆ MSG.Virus – virus name,
- ◆ MSG.Action – curing action;

Installation_Bad:

- ◆ MSG.Error – error message;

Installation_OK: no variables are available;



License_Limit – is sent when the number of registered stations is approaching the license limit, namely less than 5% of the license limit or less than two stations is unused:

- ◆ `MSG.Used` – number of stations in the base,
- ◆ `MSG.Licensed` – permitted by license,
- ◆ `GEN.StationPrimaryGroupName` – primary group name,
- ◆ `GEN.StationPrimaryGroupID` – primary group ID;

Logger_Write_Error – is sent on log write error:

- ◆ `MSG.Error` – message text;

Logger_Rotate_Error – is sent on log rotation error:

- ◆ `MSG.Error` – message text;

Low_Var_Free_Space:

- ◆ `MSG.Path` – the path to the folder with low free space,
- ◆ `MSG.FreeSpace` – free space in bytes,
- ◆ `MSG.FreeInodes` – the number of free inodes file descriptors (has the meaning only for some UNIX system-based OS),
- ◆ `MSG.RequiredSpace` – free space required for operation,
- ◆ `MSG.RequiredInodes` – number of free inodes required for operation (has the meaning only for some UNIX system-based OS);

Near_Max_Stations – is sent at every **Server** launch in case the **Server** is launched with a key allowing a lesser number of stations than it already has:

- ◆ `MSG.Used` – number of stations in the base,
- ◆ `MSG.Licensed` – permitted by license,
- ◆ `MSG.Percent` – the percentage of free licenses;

Newbie_Not_Allowed: no variables are available;

Not_Seen_For_A_Long_Time:

- ◆ `MSG.StationName` – station name,
- ◆ `MSG.StationID` – station UUID,
- ◆ `MSG.DaysAgo` – number of days since the last visit,
- ◆ `MSG.LastSeenFrom` – address the station was seen at the last visit;

Periodic_Report:

- ◆ `MSG.Attachment` - path to the report,
- ◆ `MSG.AttachmentType` - MIME type,
- ◆ `GEN.File` - report file name;

Processing_Error:

- ◆ `MSG.Component` – component name,
- ◆ `MSG.RunBy` – component is launched by this user,
- ◆ `MSG.ServerTime` – event receipt time (GMT),
- ◆ `MSG.ObjectName` – object name,
- ◆ `MSG.ObjectOwner` – object owner,
- ◆ `MSG.Error` – error message;

Rejected_Newbie:



- ◆ `MSG.AdminName` – administrator name,
 - ◆ `MSG.AdminAddress` – administrator **Dr.Web Security Control Center** address;
- Station_Already_Logged_In** – is sent, if the station is already currently registered at this or another **Server**;
- ◆ `MSG.ID` – station UUID,
 - ◆ `MSG.StationName` – name of the station,
 - ◆ `MSG.Server` – ID of the **Server** at which the station is registered;
- Station_Authorization_Failed:**
- ◆ `MSG.ID` – station UUID,
 - ◆ `MSG.Rejected` – values: `rejected` – access to a station is denied, `newbie` – there was an attempt to assign the "newbie" status to a station;
- Statistics:**
- ◆ `MSG.Component` – component name,
 - ◆ `MSG.ServerTime` – event receipt time (GMT),
 - ◆ `MSG.Scanned` – number of scanned objects,
 - ◆ `MSG.Infected` – number of infected objects,
 - ◆ `MSG.Modifications` – number of objects infected with known modifications of viruses,
 - ◆ `MSG.Suspicious` – number of suspicious objects,
 - ◆ `MSG.Cured` – number of cured objects,
 - ◆ `MSG.Deleted` – number of deleted objects,
 - ◆ `MSG.Renamed` – number of renamed objects,
 - ◆ `MSG.Moved` – number of moved objects,
 - ◆ `MSG.Speed` – processing speed in KB/s;
- Test_Message:**
- ◆ `MSG.TestMessage` – text of the test message;
- Too_Many_Stations** – is sent when a new station cannot log in on the **Server** due to the license limitations;
- ◆ `MSG.ID` – station UUID;
- Unknown_Administrator:**
- ◆ `MSG.Login` – login,
 - ◆ `MSG.Address` – network **Dr.Web Security Control Center** address;
- Unknown_Station:**
- ◆ `MSG.ID` – UUID of unknown station,
 - ◆ `MSG.Rejected` – values: `rejected` – access for a station is denied; `newbie` – there was an attempt to assign the "newbie" status to a station;
- Update_Failed:**
- ◆ `MSG.Product` – updated product,
 - ◆ `MSG.ServerTime` – (local) time of receipt of a message by the **Server**;
- Update_Wants_Reboot:**
- ◆ `MSG.Product` – updated product,
 - ◆ `MSG.ServerTime` – (local) time of receipt of a message by the **Server**.



Message Variables United According to Message Types (for Neighbor Server)

Server_Not_Seen_For_A_Long_Time - is sent if the neighbor **Server** has not been connected for a long time.

- ◆ `MSG.StationName` - the neighbor **Server** name,
- ◆ `MSG.LastDisconnectTime` - the time when the **Server** has been connected at the last time;

Too_Many_Donations - is sent when donating to the neighbor **Server** more licenses than the license key has:

- ◆ `MSG.ObjId` - license key ID;

Donation_Expired - is sent if the time of licenses donation to the neighbor **Server** has expired:

- ◆ `MSG.ObjId` - license key ID,
- ◆ `MSG.Server` - the neighbor **Server** name.

Message Variables United According to Message Types (for Server Updating Subsystem)

Srv_Repository_Cannot_flush: no variables are available;

Srv_Repository_Frozen: no variables are available;

Srv_Repository_Load_failure:

- ◆ `MSG.Reason` - message on the cause of the error;

Srv_Repository_Update:

- ◆ `MSG.AdddedCount` - number of added files,
- ◆ `MSG.ReplacedCount` - number of replaced files,
- ◆ `MSG.DeletedCount` - number of deleted files,
- ◆ `MSG.Added` - list of added files (each name in a separate line),
- ◆ `MSG.Replaced` - list of replaced files (each name in a separate line),
- ◆ `MSG.Deleted` - list of deleted files (each name in a separate line);

Srv_Repository_UpdateFailed:

- ◆ `MSG.Error` - error message,
- ◆ `MSG.ExtendedError` - detailed description of the error;

Srv_Repository_UpToDate: no variables are available.



The variables of the last template do not include the files marked as "not to be notified of" in the product configuration file, read [F1. The Syntax of the Configuration File .config](#).

The variables of the Server messages about the coming license expiration

Key_Expiration:

- ◆ `MSG.Expiration` - date of license expiration,
- ◆ `MSG.Expired` - 1, if the term has expired, otherwise 0,
- ◆ `MSG.ObjId` - object GUID,
- ◆ `MSG.ObjName` - object name,
- ◆ `MSG.ObjType` - object using an expiring key (server/station/group).



Appendix E. The Specification of Network Addresses

In the specification the following conventions are taken:

- ◆ variables (the fields to be substituted by concrete values) are enclosed in angle brackets and written in italic,
- ◆ permanent text (remains after substitutions) is written in bold,
- ◆ optional elements are enclosed in brackets,
- ◆ the defined notion is placed on the left of the `:=` character string, and the definition is placed on the right (as in the Backus-Naur form).

E1. The General Format of Address

The network address looks as follows:

[*<protocol>*/] [*<protocol-specific-part>*]

By default, *<protocol>* has the TCP value. The default values of *<protocol-specific-part>* are determined by the application.

IP Addresses

- ◆ *<interface>* := *<ip-address>*
<ip-address> can be either a DNS name or an IP address separated by periods (for example, 127.0.0.1).
- ◆ *<socket-address>* := *<interface>* : *<port-number>*
<port-number> must be specified by a decimal number.

Examples:

1. `tcp/127.0.0.1:2193`

means a TCP protocol, port 2193 on an interface 127.0.0.1.

2. `tcp/[::]:2193`

means a TCP protocol, port 2193 on an IPv6 interface 0000.0000.0000.0000.0000.0000.0000.0000

3. `localhost:2193`

the same.

4. `tcp/:9999`

value for the **Server**: the default interface depending on the application (usually all available interfaces), port 9999; value for client: the default connection to the host depending on the application (usually localhost), port 9999.

5. `tcp/`

TCP protocol, default port.

UDS Addresses

- ◆ Connection-oriented protocol:
`unx/<file_name>`



- ◆ Datagram-oriented protocol:

`udx/<file_name>`

Examples:

1. `unx/tmp/drwcsd:stream`
2. `unx/tmp/drwcsd:datagram`

Connection-Oriented Protocol

`<protocol>/<socket-address>`

where `<socket-address>` sets the local address of the socket for the **Server** or a remote server for the client.

Datagram-Oriented Protocol

`<protocol>/<endpoint-socket-address>[-<interface>]`

Examples:

1. `udp/231.0.0.1:2193`

means using a multicast group `231.0.0.1:2193` on an interface depending on the application by default.

2. `udp/[ff18::231.0.0.1]:2193`

means using a multicast group `[ff18::231.0.0.1]` on an interface depending on the application by default.

3. `udp/`

application-dependent interface and endpoint.

4. `udp/255.255.255.255:9999-myhost1`

using broadcasting messages on port `9999` on `myhost1` interface.

SRV Addresses

`srv/[<server name>][@<domain name/dot address>]`

E2. The Addresses of Dr.Web Server

Receipt of Connections

`<connection-protocol>/[<socket-address>]`

By default, depending on `<connection-protocol>`:

- ◆ `tcp/0.0.0.0:2193`

which means "all interfaces (excluding those with IPv6 addresses), port 2193";

- ◆ `tcp/[::]:2193`

which means "all IPv6 addresses, port 2193".



Dr.Web Server Location Service

`<datagram-protocol>/ [<endpoint-socket-address> [-<interface>]]`

By default, depending on `<datagram-protocol>`:

- ◆ `udp/231.0.0.1:2193-0.0.0.0`
which means using a multicast group `231.0.0.1:2193` for all interfaces;
- ◆ `udp/[ff18::231.0.0.1]:2193-[::]:0`
which means using a multicast group `[ff18::231.0.0.1:2193]` on all interfaces.

E3. The Addresses of Dr.Web Agent/ Installer

Direct Connection to Dr.Web Server

`[<connection-protocol>] / [<remote-socket-address>]`

By default, depending on `<connection-protocol>`:

- ◆ `tcp/127.0.0.1:2193`
means loopback port `2193`,
- ◆ `tcp/[::]:2193`
means loopback port `2193` for IPv6.

`<drwcs-name>` Dr.Web Server Location Using the Given Family of Protocols and Endpoint

`[<drwcs-name>] @ <datagram-protocol> / [<endpoint-socket-address> [-<interface>]]`

By default, depending on `<datagram-protocol>`:

- ◆ `drwcs@udp/231.0.0.1:2193-0.0.0.0`
location of a **Server** with the `drwcs` name for a TCP connection using a multicast group `231.0.0.1:2193` for all interfaces.



Appendix F. Administration of the Repository



It is recommended to manage repository via the corresponding settings of the **Control Center**. For more details, see **Administrator Manual**, p. [Administration of Dr.Web Server Repository](#).

Repository settings are saved to the following repository configuration files:

- [General configuration files](#) reside in the root folder of the repository and specify parameters of update servers.
- [Products configuration files](#) reside in the root folders that correspond to concrete repository products and specify the files set and update settings for the product in the folder of which they are located.



After the configuration files have been edited, restart the **Server**.



When setting up interserver links for product mirroring (see **Administrator Manual**, p. [Peculiarities of a Network with Several Dr.Web Servers](#)), please remember that configuration files are not the part of the product and therefore are not properly handled by the mirror system. To avoid errors during the updating

- ◆ for peer **Servers**, use identical configuration,
- ◆ for subordinate **Servers**, disable synchronizing of components through HTTP protocol or keep the configuration identical.

F1. General configuration files

.servers

The `.servers` file contains the list of servers for updating the components of **Dr.Web Enterprise Security Suite** in the **Dr.Web Server** repository from the **GUS** servers.

The servers in the list are polled consequently, once the updating is successful, the polling procedure terminates.

For Example:

```
esuite.geo.drweb.com
esuite.msk3.drweb.com
esuite.msk4.drweb.com
esuite.msk.drweb.com
esuite.us.drweb.com
esuite.jp.drweb.com
```

.url

The `.url` file contains the base URI of updates zone - the folder on updates servers that contains updates of concrete **Dr.Web** product.

**For Example:**

```
update
```

.auth

The `.auth` file contains parameters of user authorization on the update server.

Authorization parameters are specified in the following format:

```
<user name>  
<password>
```

User name is mandatory, password is optional.

For Example:

```
admin  
root
```

.delivery

The `.delivery` file contains settings for transferring updates from the **GUS** servers.

Parameter	Possible values	Description
<code>cdn</code>	<code>on</code> <code>off</code>	Using Content Delivery Network during repository loading: <ul style="list-style-type: none">• <code>on</code> - use CDN,• <code>off</code> - do not use CDN.
<code>cert</code>	<code>drweb</code> <code>valid</code> <code>any</code> <code>custom</code>	Allowed SSL certificates of update servers that will be automatically accepted: <ul style="list-style-type: none">• <code>drweb</code> - accept only SSL certificate of Doctor Web company,• <code>valid</code> - accept only valid SSL certificates,• <code>any</code> - accept any certificates,• <code>custom</code> - accept certificate defined by user.
<code>cert-path</code>		Path to the user-defined if the <code>custom</code> mode of the <code>cert</code> parameter is set.
<code>ssh-mode</code>	<code>pwd</code> <code>pubkey</code>	Authorization mode when using <code>scp</code> and <code>sftp</code> protocols (based on <code>ssh2</code>): <ul style="list-style-type: none">• <code>pwd</code> - authorization by user login and password,• <code>pubkey</code> - authorization by encryption keys.
<code>ssh-pubkey</code>		Path to the public ssh key of update server.
<code>ssh-prikey</code>		Path to the private ssh key of update server.



F2. Products configuration files

.description

The `.description` file sets a product name. If the file is absent, the name of the respective folder of the product is used as the product name.

For Example:

```
Dr.Web Server
```

.sync-off

The file disables the product update. Content is irrelevant.

Files of Exclusions in Updating the Server Repository from the GUS

.sync-only

The `.sync-only` file contains the regular expressions that define the list of repository files which will be synchronized during update of the repository from the **GUS**. Repository files not specified in the `.sync-only`, will not be synchronized. If the `.sync-only` file is absent, all repository files will be synchronized except those files which are excepted according to the settings in the `.sync-ignore` file.

.sync-ignore

The `.sync-ignore` file contains the regular expressions that define the list of repository files which will be excluded from synchronization during update of the repository from the **GUS**.

Example of the file with exceptions:

```
^windows-nt-x64/  
^windows-nt/  
^windows/
```

The Order of Use of Configuration Files

If the `.sync-only` and `.sync-ignore` files are present for the product, the following scheme of actions is used:

1. The `.sync-only` is applied first. Files not listed in the `.sync-only`, are not handled.
2. To the rest of files, the `.sync-ignore` is applied.



Files of Exclusions in Updating the Agents from the Server

.state-only

The `.state-only` file contains the regular expressions that define the list of repository files which will be synchronized during update of the **Agents** from the **Server**. Repository files not specified in the `.state-only`, will not be synchronized. If the `.state-only` file is absent, all repository files will be synchronized except those files which are excepted according to the settings in the `.state-ignore` file.

.state-ignore

The `.state-ignore` file contains the regular expressions that define the list of repository files which will be excluded from synchronization during update of the **Agents** from the **Server**.

For Example:

- ◆ German, Polish and Spanish interface languages should not be received (others - will be received),
- ◆ no components designed for Windows OS 64-bit should be received.

```
;^common/ru-.*\.dwl$ this will be updated
^common/de-.*\.dwl$
^common/pl-.*\.dwl$
^common/es-.*\.dwl$
^win/de-.*
^win/pl-.*
^windows-nt-x64\.*
```

The order of using `.state-only` and `.state-ignore` is the same as for the `.sync-only` and `.sync-ignore`.

Notification Sending Configuration

The files of the `notify` group allow to configure the notification system on successful update of the separate products ().



These settings are refer the **Product has been updated** notification only. To all other notification types, exceptions are not applied.

The setting of the notification system is described in **Administrator Manual**, p. [Setting Notifications](#).

.notify-only

The `.notify-only` file contains the list of repository files on changing of which the notification will be sent.



.notify-ignore

The `.notify-ignore` file contains the list of repository files on changing of which the notification will not be sent.

The Order of Use of Configuration Files

If the `.notify-only` and `.notify-ignore` files are present for the product, the following scheme of actions is used:

1. At product update, files updates from the **GUS**, are compared with exclusions list.
2. Files included into the `.notify-ignore` list, are excluded first.
3. From the rest of files, whose are excluded which are not in the `.notify-only` list.
4. If files not excluded on the previous steps are remained, notifications will be sent.

If the `.notify-only` and `.notify-ignore` files are absent, notifications will be always sent (if they are enabled on the **Notifications configuration** page in the **Control Center**).

For Example:

If in the `.notify-ignore` file, the `^.vdb.lzma$` exception is set, and only virus databases are updated, notification will not be sent. If the `drweb32.dll` engine is updated with the databases, when notification will be sent.

Freeze Settings

.delay-config

The `.delay-config` file contains settings to disable switching the product to the new revision. Repository continues distributing the previous revision, and synchronization is no longer performed (the state of the product become "frozen"). If administrator decides that received revision is adequate for distributing, administrator must enable its distribution in the **Control Center** (see **Administrator Manual**, p. [Administration of Dr.Web Server Repository](#)).

The file contains two not case sensitive parameters which are separated by a semicolon.

File format:

```
Delay [ON|OFF]; UseFilter [YES|NO]
```

Parameter	Possible values	Description
Delay	ON OFF	<ul style="list-style-type: none"> • ON - freeze of product updates is enabled. • OFF - freeze of product updates is disabled.
UseFilter	YES NO	<ul style="list-style-type: none"> • Yes - freeze updates only if updates files match the exceptions list in the <code>.delay-only</code> file. • No - freeze updates in any case.

For Example:

```
Delay ON; UseFilter NO
```



.delay-only

The `.delay-only` file contains the list of files, changing of which disables the switching the product on a new revision. The list of files is set in a regular expressions format.

If the file from the repository update meets the specified masks and the `UseFilter` setting in the `.sync-only` file if enabled, when revision will be frozen.

.rev-to-keep

The `.rev-to-keep` file contains the number of stored product revisions.

For Example:

```
3
```




Appendix G. Configuration Files

This section describes the format of the following files:

- ◆ `drwcsd.conf` configuration file of **Dr.Web Server**;
- ◆ `drwcsd-proxy.xml` configuration file of the **Proxy server**;
- ◆ `webmin.conf` configuration file of **Dr.Web Security Control Center**;
- ◆ `download.conf` configuration file.



If on the computer with corresponding component, the **Agent** with enabled self-protection is installed, before editing configuration files, disable **Dr.Web Self-protection** component via the **Agent** settings.

After you save all changes, it is recommended to enable **Dr.Web Self-protection** component.

G1. Dr.Web Server Configuration File

The `drwcsd.conf` **Server** configuration file resides by default in the `etc` subfolder of the **Server** root folder. If the **Server** is run with a command line parameter, a non-standard location and name of the configuration file can be set (for more read Appendix [H4. Dr.Web Server](#)).

To manage Dr.Web Server configuration file manually, do the following:

1. Stop the **Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
2. Disable self-protection (in case of installed **Agent** with the active self-protection - in the **Agent** context menu).
3. Manage the **Server** configuration file.
4. Start the **Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).

Dr.Web Server Configuration File Format

Server configuration file is in XML format.

Description of Dr.Web Server configuration file parameters:

```
o <version value='10'>
```

Current version of **Dr.Web Server**.

```
◆ <name value=''>
```

The name of **Dr.Web Server** or a cluster of **Dr.Web Servers**, which is used during the search by **Agent**, **Agent** installers and **Control Center**. Leave the value blank (" is used by default), to use the name of the computer where **Dr.Web Server** software is installed.

```
◆ <id value=''>
```

The **Сервера** unique identifier. In the previous versions was placed in the **Server** license key. Starting from version **10**, is stored in the **Server** configuration file.

```
◆ <location city='' country='' department='' floor='' latitude='' longitude='' organization='' province='' room='' street=''>
```

The **Server** geographic location.

Attributes description:

Attribute	Description
city	City



Attribute	Description
country	Country
department	Department name
floor	Floor
latitude	Latitude
longitude	Longitude
organization	Organization name
province	Province name
room	Room number
street	Street name

◆ `<threads count=''/>`

The threads number processing data from the **Agents**. Minimal value is 5. Default is 5. This parameter affects **Server** performance. Change the default setting on advice of the technical support only.

◆ `<newbie approve-to-group='' default-rate='' mode=''/>`

Access mode for new stations.

Attributes description:

Attribute	Allowed values	Description	Default
approve-to-group	-	The group which is set as a primary by default for new stations for the Allow access automatically (<code>mode='open'</code>).	Empty value, which means assign the Everyone group as a primary.
default-rate	-	For AV-Desk . The group which is set as a tariff by default for new stations for the Allow access automatically (<code>mode='open'</code>).	Empty value, which means assign the Dr.Web Premium group as a tariff.
mode	<ul style="list-style-type: none"> open - allow access automatically, closed - always deny access, approval - approve access manually. 	New stations approval policy.	-

For more details see **Administrator Manual**, p. [New Stations Approval Policy](#).

◆ `<unauthorized-to-newbie enabled=''/>`

Policy of actions on unauthorized stations. Allowed values of `enabled`:

- yes - stations authorization of which is failed (e.g., if the database is corrupted), will be automatically reset to newbies,
- no (default) - normal operation mode.

◆ `<maximum-authorization-queue size=''/>`

Maximal number of stations in the queue for authorization on the **Server**. Change the default setting on advice of the technical support only.

◆ `<reverse-resolve enabled=''/>`

Replace IP address with DNS names in **Dr.Web Server** log file. Allowed values of `enabled`:

- yes - show DNS names.



- no (Default) - show IP addresses.

◆ `<replace-netbios-names enabled='' />`

Replace NetBIOS names of computers with DNS names. Allowed values of `enabled`:

- yes - show DNS names.
- no (Default) - show NetBIOS names.

◆ `<dns>`

DNS settings.

`<timeout value='' />`

Timeout in seconds for resolving DNS direct/reverse queries. Leave the value blank to disable restriction on wait time until the end of the resolution

`<retry value='' />`

Maximum number of repeated DNS queries on fail while resolving the DNS query.

`<cache enabled='' negative-ttl='' positive-ttl='' />`

Time for storing responses from DNS server in the cache.

Attributes description:

Attribute	Allowed values	Description
enabled	<ul style="list-style-type: none"> • yes - store responses in the cache, • no - do not store responses in the cache. 	Mode of storing responses in the cache.
negative-ttl	-	Storage time in the cache (TTL) of negative responses from the DNS server in minutes.
positive-ttl	-	Storage time in the cache (TTL) of positive responses from the DNS server in minutes.

`<servers>`

List of DNS servers, which replaces default system list. Contains one or several `<server address="" />` child elements, the `address` parameter of which defines IP address of the server.

`<domains>`

List of DNS domains, which replaces default system list. Contains one or several `<domain name="" />` child elements, the `name` parameter of which defines the domain name.

◆ `<cache>`

Caching settings.

The `<cache />` element contains the following child elements:

- `<interval value='' />`

Period of full cache flush in seconds.

- `<quarantine ttl='' />`

Cleanup interval of **Server** quarantined files in seconds. Default is 604800 (one week).

- `<download ttl='' />`

Cleanup interval of personal installation packages. Default is 604800 (one week).

- `<repository ttl='' />`

Cleanup interval of files in the **Server** repository in seconds.

- `<file ttl='' />`

Cleanup interval of file cache in seconds. Default is 604800 (one week).

◆ `<replace-station-description enabled='' />`

Synchronize stations descriptions on **Dr.Web Server** with the **Computer description** field at the **System properties** page on the station. Allowed values of `enabled`:



- yes - replace description on the **Server** with description on the station.
- no (Default) - ignore description on station.

◆ `<time-discrepancy value='' />`

Allowed difference between system time at **Dr.Web Server** and **Dr.Web Agents** in minutes. If the difference is larger than specified value, it will be noted in the status of the station at **Dr.Web Server**. 3 minutes are allowed by default. The empty value or the 0 value means that checking is disabled.

◆ `<encryption mode='' />`

Traffic encryption mode. Allowed values of `mode`:

- yes - use encryption,
- no - do not use encryption,
- possible - encryption is allowed.

Default is yes.

For more details see **Administrator Manual**, p. [Traffic Encryption and Compression](#).

◆ `<compression level='' mode='' />`

Traffic compression mode.

Attributes description:

Attribute	Allowed values	Description
level	Integer from 1 to 9.	Compression level.
mode	<ul style="list-style-type: none"> • yes - use compression, • no - do not use compression, • possible - compression is allowed. 	Compression mode.

For more details see **Administrator Manual**, p. [Traffic Encryption and Compression](#).

◆ `<track-agent-jobs enabled='' />`

Allow monitoring and storing into the **Server** database the results of tasks execution on workstations. Allowed values of `enabled`: yes or no.

◆ `<track-agent-status enabled='' />`

Allow monitoring of changes in the stations state and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<track-virus-bases enabled='' />`

Allow monitoring of changes in the state (compound, changes) of virus bases on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no. Параметр игнорируется, если `<track-agent-status enabled='no' />`.

◆ `<track-agent-modules enabled='' />`

Allow monitoring of modules versions on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<track-agent-components enabled='' />`

Allow monitoring of the list of installed components on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<track-agent-userlogon enabled='' />`

Allow monitoring of user sessions on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<track-agent-environment enabled='' />`



Allow monitoring of compound of hardware and software on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<keep-run-information enabled='' />`

Allow monitoring of information on start and stop of anti-virus components operating on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<keep-infection enabled='' />`

Allow monitoring of threats detection on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<keep-scan-errors enabled='' />`

Allow monitoring of scan errors on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<keep-scan-statistics enabled='' />`

Allow monitoring of scan statistics on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<keep-installation enabled='' />`

Allow monitoring of information on **Agent** installations on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<quarantine enabled='' />`

Allow monitoring of information on the **Quarantine** state on stations and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<update-bandwidth queue-size='' value='' />`

Maximal network traffic bandwidth in KB/sec. for transmitting updates from **Server** to **Agents**.

Attributes description:

Attribute	Allowed values	Description	Default
queue-size	<ul style="list-style-type: none"> positive integer, unlimited. 	Maximum allowable number of updates distribution sessions running at the same time from the Server . When the limit is reached, the Agent requests are placed into the waiting queue. The waiting queue size is unlimited.	unlimited
value	<ul style="list-style-type: none"> maximal speed in KB/sec, unlimited. 	Maximal summary speed for updates transmission.	unlimited

◆ `<install-bandwidth queue-size='' value='' />`

Maximal network traffic bandwidth in KB/sec. for transmitting data during **Dr.Web Agent** installation on stations.

Attributes description:

Attribute	Allowed values	Description	Default
queue-size	<ul style="list-style-type: none"> positive integer, unlimited. 	Maximum allowable number of the Agent installation sessions running at the same time from the Server . When the limit is reached, the Agent requests are placed into the waiting queue. The waiting queue size is unlimited.	unlimited
value	<ul style="list-style-type: none"> maximal speed in KB/sec, unlimited. 	Maximal summary speed for transmitting data during Agent installations.	unlimited

◆ `<geolocation enabled='' startup-sync='' />`



Enable synchronization of stations geolocation between **Dr.Web Servers**.

Attributes description:

Attribute	Allowed values	Description
enabled	<ul style="list-style-type: none"> yes - allow synchronization, no - disable synchronization. 	Synchronization mode.
startup-sync	Positive integer.	Number of stations without geographical coordinates, information on which is requested when establishing a connection between Dr.Web Servers .

◆ `<audit enabled=''/>`

Allow monitoring of administrator operations in **Dr.Web Security Control Center** and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<audit-internals enabled=''/>`

Allow monitoring of internal operations in **Dr.Web Server** and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<audit-xml-api enabled=''/>`

Allow monitoring of operations via Web API in **Dr.Web Server** and storing the information into the **Server** database. Allowed values of `enabled`: yes or no.

◆ `<proxy enabled='no' host='' password='' user=''/>`

Parameters of connections to **Dr.Web Server** via HTTP proxy server.

Attributes description:

Attribute	Allowed values	Description
enabled	<ul style="list-style-type: none"> yes - use proxy server, no - do not use proxy server. 	Mode of connections to Dr.Web Server via HTTP proxy server.
host	-	Proxy server address.
password	-	Password of proxy server user if proxy server requires authorization.
user	-	Name of proxy server user if proxy server requires authorization.

◆ `<statistics enabled='' id='' interval=''/>`

Parameters of sending of the statistics on virus events to the **Doctor Web** company to the stat.drweb.com section.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	<ul style="list-style-type: none"> yes - send statistics, no - do not send statistics. 	Mode of statistics sending to the Doctor Web company.	-
id	-	MD5 of the Agent license key.	-
interval	Positive integer.	Interval of statistics sending in minutes.	30

◆ `<cluster>`

Parameters of **Dr.Web Servers** cluster for data exchange in multiserver anti-virus network configuration

Contains one or several `<on multicast-group="" port="" interface=""/>` child elements.

Attributes description:



Attribute	Description
multicast-group	IP address of multicast group through which Servers will be exchange information.
port	Port number of network interface to which transport protocol is bound to transmit the information into multicast group.
interface	IP address of network interface to which transport protocol is bound to transmit the information into multicast group.

◆ `<mcast-updates enabled="">`

Configuration of updates transmission on workstations via the multicast protocol. Allowed values of `enabled`: yes OR no.

The `<mcast-updates />` element contains one or several `<on multicast-group="" port="" interface="" />` child elements.

Attributes description:

Attribute	Description
multicast-group	IP address of multicast group in which stations receive multicast updates.
port	Port number of Dr.Web Server network interface, to which transport multicast protocol is bound for updates transmission. <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">  For multicast updates, you must specify any unused port, particularly, different from the port that is specified in the settings of transport protocol for Server operating. </div>
interface	IP address of Dr.Web Server network interface, to which transport multicast protocol is bound for updates transmission

The `<mcast-updates />` element contains the `<transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" />` child element.

Attributes description:

Attribute	Description	Default
datagram-size	UDP datagram size (bytes) - size of UDP datagrams in bytes. Allowed range is 512 - 8192. To avoid fragmentation, it is recommended to set a value less than MTU (Maximum Transmission Unit) of the network.	4096
assembly-timeout	File transmission time (ms.) - during specified time, single update file is transmitted, after that Server starts sending the next file. All files which failed to transmit at the step of multicast protocol update, will be transmitted at standard update process over the TCP protocol.	180000
updates-interval	Multicast updates duration (ms.) - duration of update process via multicast protocol. All files that failed to transmit during update stage via multicast protocol will be transmitted in process of standard update via TCP protocol.	600000
chunks-interval	Packages transmission interval (ms.) - interval of packages transmission to a multicast group. The low interval value may cause significant losses during package transfer and network overload. It is not recommended to change this parameter.	20
resend-interval	Interval between retransmission requests (ms.) - with this interval Agents send requests for retransmission of lost packages. Server accumulates these requests after that sends lost blocks.	1000



Attribute	Description	Default
silence-interval	"Silence" interval on the line (ms.) - when a file transmission is over before allowed time has expired, if during specified "silence" interval no requests from Agents for retransmission of lost packages are received, Server considers that all Agent received updates files and starts sending the next file.	10000
accumulate-interval	Retransmission requests accumulation interval (ms.) - during specified interval, Server accumulates requests from Agents for retransmission of lost packages. Agent request lost packages. Server accumulates these requests during specified time slot after that sends lost blocks.	2000

◆ `<database connections=' '>`

Database definition. The `connections` parameter specifies the number of connections of database with the **Server**. Default is 2. Change the default setting on advice of the technical support only.

The `<database />` element contains on of the following child elements:



The `<database />` element can contain only one child element defining specific database.

Database attributes that may present in the configuration file template but not described are not recommended to change without the consent of the technical support service of **Doctor Web** company.

- `<sqlite dbfile="database.sqlite" cache="SHARED" cachesize="2048" readuncommitted="off" precompiledcache="1024" serialize="yes" synchronous="FULL" openmutex="FULL" debug="no" />`

Defines SQLite3 embedded database.

Attributes description:

Attribute	Allowed values	Description	Default
dbfile		Database name.	
cache	SHARED PRIVATE	Caching mode.	SHARED
cachesize	Positive integer.	Database cache size (in 1.5Kb pages).	2048
precompiledcache	Positive integer.	Cache size of precompiled sql operators in kilobytes.	1024
synchronous	<ul style="list-style-type: none"> • TRUE or FULL - synchronous • FALSE or NORMAL - normal • OFF - asynchronous 	Data write mode.	FULL

- `<intdb dbfile="database.dbs" cachesize="2048" synchronous="FULL" />`

Defines InitDB embedded database (based on SQLite2).

Attributes description:

Attribute	Allowed values	Description	Default
dbfile		Database name.	
cachesize	Positive integer.	Database cache size (in 1.5Kb pages).	2048
synchronous	<ul style="list-style-type: none"> • TRUE or FULL - synchronous • FALSE or NORMAL - normal 	Data write mode.	FULL



Attribute	Allowed values	Description	Default
	<ul style="list-style-type: none"> • OFF - asynchronous 		

- `<pgsql dbname="drwcs" host="localhost" port="5432" options="" requiressl="" user="" password="" temp_tablespaces="" default_transaction_isolation="" debugproto="yes"/>`

Defines PostgreSQL external database.

Attributes description:

Attribute	Allowed values	Description	Default
dbname		Database name.	
host		PostgreSQL server host or path to UNIX domain socket.	
port		PostgreSQL server port or extension of UNIX domain socket file.	
options		Command line parameters to send to a database server. For more details, see chapter 18 at http://www.postgresql.org/docs/9.1/static/libpq-connect.html	
requiressl	<ul style="list-style-type: none"> • 1 0 (via Control Center) • y n • yes no • on off 	Allow SSL connections only.	<ul style="list-style-type: none"> • 0 • y • yes • on
user		Database user name.	
password		Database user password.	
temp_tablespaces		Namespace for temporary tables.	
default_transaction_isolation	<ul style="list-style-type: none"> • read uncommitted • read committed • repeatable read • serializable 	Transaction isolation level.	read committed

- `<oracle connectionstring="" user="" password="" client="" />`

Defines Oracle external database.

Attributes description:

Attribute	Description
connectionstring	String with Oracle SQL Connect URL or Oracle Net keyword-value pairs.
user	Registration name of database user.
password	Database user password.
client	Path to the Oracle Instant Client for the access to the Oracle DB. Dr.Web Server is supplied with the Oracle Instant Client of 11 version. But, for newer Oracle Servers or if the Oracle driver contains errors, you can download corresponding driver from the Oracle site and set the path to the driver in this field.

- `<odbc dsn="drwcs" user="" pass="" transaction="DEFAULT" />`

Defines connection to an external database via ODBC.



Attributes description:

Attribute	Allowed values	Description	Default
dsn		ODBC data source name.	drwcs
user		Registration name of database user.	drwcs
pass		Database user password.	drwcs
limit	Positive integer.	Reconnect to the DBMS after specified number of transaction.	0 - do not reconnect
transaction	<ul style="list-style-type: none"> SERIALIZABLE - serializable READ_UNCOMMITTED - read uncommitted data READ_COMMITTED - read committed data REPEATABLE_READ - repeatable read DEFAULT - equal "" - depends on DBMS. 	<p>Transaction isolation level.</p> <p>Some DBMS support READ_COMMITTED only.</p>	DEFAULT

◆ `<acl>`

Access control lists. Allows to configure restrictions for network addresses from which **Agents**, network installers and other (neighboring) **Dr.Web Servers** will be able to access the **Server**.

The `<acl />` element contains the following child elements into which limitations for corresponding connection types are configured:

- `<install />` - the list of limitations on IP addresses from which **Dr.Web Agents** installers can connect to this **Server**.
- `<agent />` - the list of limitations on IP addresses from which **Dr.Web Agents** can connect to this **Server**.
- `<links />` - the list of limitations on IP addresses from which neighbor **Dr.Web Servers** can connect to this **Server**.
- `<discovery />` - the list of limitations on IP addresses from which broadcast queries can be received by the *Server Detection Service*.

All child elements contain the same structure of nested elements that defines the following limitations:

- `<priority mode="">`

Lists priority. Allowed values of `mode`: "allow" or "deny". For the `<priority mode="deny">` value, the `<deny />` list has a higher priority than the `<allow />` list. Addresses not included in any of the lists or included into both of them are denied. Allowed only addresses that are included in the `<allow />` list and not included in the `<deny />` list.

- `<allow />`

The list of TCP addresses from which the access is allowed. The `<allow />` element contains one or several `<ip address="" />` child elements to specify allowed addresses in the IPv4 format and `<ip6 address="" />` to specify allowed addresses in the IPv6 format. The attribute `address` defines network addresses in the following format: `<IP address>/[<prefix>]`.

- `<deny />`



The list of TCP addresses from which the access is denied. The `<deny />` element contains one or several `<ip address="" />` child elements to specify denied addresses in the IPv4 format and `<ip6 address="" />` to specify denied addresses in the IPv6 format. The attribute `address` defines network addresses in the following format: `<IP address>/[<prefix>]`.

◆ `<scripts profile='' stack='' trace='' />`

Scripts profiling parameters configuration.

Attributes description:

Attribute	Allowed values	Description	Default
profile		Log information on Server scripts execution profiling. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.	
stack	<ul style="list-style-type: none"> • yes, • no. 	Log information on Server scripts execution from a call stack. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.	no
trace		Log information on Server scripts execution tracing. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.	

◆ `<lua-module-path>`

Lua interpreter paths.



The paths order is important.

The `<lua-module-path />` element contains the following child elements:

- `<cpath root='' />` - path to the binary modules folder. Allowed values of `root`: `home` (default), `var`, `bin`, `lib`.
- `<path value='' />` - path to the scripts folder. If it is not a child of the `<jobs />` or `<hooks />` elements, when it is used by both. Paths specified in the `value` attribute, are relative from paths in the `root` attribute of the `<cpath />` element.
- `<jobs />` - paths for tasks from the **Server** schedule.

The `<jobs />` element contains one or several `<path value='' />` child elements to specify the path to the scrips folder.

- `<hooks />` - пути для пользовательских процедур **Сервера**.

The `<hooks />` element contains one or several `<path value='' />` child elements to specify the path to the scrips folder.

◆ `<trandports>`

Configuration of transport protocols parameters used by the **Server** to connect with clients. Contains one or several `<trandport discovery='' ip='' name='' multicast='' multicast-group='' port='' />` child elements.

Attributes description:

Attribute	Description	Obligatory	Allowed values	Default
discovery	Defines whether the Server detection service is used or not.	no, specified with the <code>ip</code> attribute only.	yes, no	no
<ul style="list-style-type: none"> • ip • unix 	Defines the family of used protocols and specifies the interface address.	yes	-	<ul style="list-style-type: none"> • 0.0.0.0 • -
name	Specifies the Server name for the Server detection service.	no	-	drwcs



Attribute	Description	Obligatory	Allowed values	Default
multicast	Defines whether the Server included into a multicast group or not.	no, specified with the <code>ip</code> attribute only.	yes, no	no
multicast-group	Specifies the address of the multicast group into which the Server is included.	no, specified with the <code>ip</code> attribute only.	-	<ul style="list-style-type: none"> • 231.0.0.1 • [ff18::231.0.0.1]
port	Port to listen.	no, specified with the <code>ip</code> attribute only.	-	2193

◆ `<protocols>`

The list of disabled protocols. Contains one or several `<protocol enabled='' name=''>` child elements.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	<ul style="list-style-type: none"> • yes - protocol is enabled, • no - protocol is disabled. 	Protocol usage mode.	no
name	<ul style="list-style-type: none"> • AGENT - protocol that allows interaction of the Server with Dr.Web Agents. • MSNAPSHV - protocol that allows interaction of the Server with the Microsoft NAP Validator component of system health validating. • INSTALL - protocol that allows interaction of the Server with Dr.Web Agent installers. • CLUSTER - protocol for interaction between Servers in the cluster system. • SERVER - protocol that allows interaction of the Dr.Web Server with other Dr.Web Servers. 	Protocol name.	-

◆ `<plugins>`

The list of disabled extensions. Contains one or several `<plugin enabled='' name=''>` child elements.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	<ul style="list-style-type: none"> • yes - extension is enabled, • no - extension is disabled. 	Extension usage mode.	no
name	<ul style="list-style-type: none"> • WEBMIN - Dr.Web Security Control Center extension for managing the Server and anti-virus network via the Control Center. • FrontDoor - Dr.Web Server FrontDoor extension that allows connections of Server remote diagnostics utility. 	Extension name.	-

◆ `<license-exchange>`

Settings of licenses propagation between **Dr.Web Servers**.

The `<license-exchange />` element contains the following child elements:

- `<expiration-interval value=''>`
- `<prolong-preact value=''>`
- `<check-interval value=''>`



Elements description:

Element	Description	The value attribute default values, min.
expiration-interval	Validity period of donated licenses - time period on which licenses are donated from the key on this Server . The setting is used if the Server donates licenses to neighbor Servers.	1440
prolong-preact	Period for accepted licenses renewal - period till the license expiration, starting from which this Server initiates renewal of the license which is accepted from the neighbor Server . The setting is used if the Server accepts licenses from neighbor Servers .	60
check-interval	License synchronization period - interval for synchronizing information about donating licenses between Servers .	1440

◆ `<email from="" debug="">`

Parameters of sending emails from the **Control Center**, e.g., as administrative notifications or when mailing installation packages of the stations.

Attributes description:

Attribute	Allowed values	Description	Default
from	-	Email address which will be set as a sender of emails.	drwcs@localhost
debug	<ul style="list-style-type: none"> yes - use debug mode, no - do not use debug mode. 	Use debug mode to get SMTP session detailed log.	no

The `<email />` element contains the following child elements:

- `<smtp server="" user="" pass="" port="" start_tls="" auth_plain="" auth_login="" auth_cram_md5="" auth_digest_md5="" auth_ntlm="" conn_timeout=""/>`

SMTP server parameters configuration to send emails.

Attributes description:

Attribute	Allowed values	Description	Default
server	-	SMTP server address which is used to send emails.	127.0.0.1
user	-	name of SMTP server user, if the SMTP server requires authorization.	-
pass	-	password of SMTP server user, if the SMTP server requires authorization.	-
port	Positive integer.	SMTP server port which is used to send emails.	25
start_tls		Use <i>STARTTLS</i> traffic encoding for sending emails.	yes
auth_plain		Use <i>plain text</i> authentication on a mail server.	no
auth_login	<ul style="list-style-type: none"> yes - use this authentication type, 	Use <i>LOGIN</i> authentication on a mail server.	no
auth_cram_md5	<ul style="list-style-type: none"> no - do not use this authentication type. 	Use <i>CRAM-MD5</i> authentication on a mail server.	no
auth_digest_md5		Use <i>DIGEST-MD5</i> authentication on a mail server.	no
auth_ntlm		Use <i>AUTH-NTLM</i> authentication on a mail server.	no



Attribute	Allowed values	Description	Default
conn_timeout	Positive integer.	Connection timeout for SMTP server.	180

• `<ssl enabled="" verify_cert="" ca_certs=""/>`

SSL traffic encryption parameters configuration for sending emails.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	<ul style="list-style-type: none"> yes - use SSL, no - do not use SSL. 	SSL encryption usage mode.	no
verify_cert	<ul style="list-style-type: none"> yes - check SSL certificate, no - do not check SSL certificate. 	Validate the SSL certificate of a mail server.	no
ca_certs	-	The path to the root SSL certificate of Dr.Web Server .	-

◆ `<track-epidemic enabled='' period='' threshold=''/>`

Configuration of parameters for tracking virus epidemic in the network.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	<ul style="list-style-type: none"> yes - enable epidemic tracking and send single notification on threats, no - disable epidemic tracking and send notifications on threats in normal mode. 	Administrator notification mode on virus epidemic.	no
period	Positive integer.	Time period in seconds, during which specified number of messages on infections must be received, so that Dr.Web Server may send to the administrator a single notification on epidemic on all cases of infection.	300
threshold		The number of messages on infections that must be received in specified time period, so that Dr.Web Server may send to the administrator a single notification on epidemic on all cases of infection.	100

G2. Dr.Web Security Control Center Configuration File

The `webmin.conf` **Dr.Web Security Control Center** configuration file is in XML format and located in the `etc` subfolder of **Server** root folder.

Description of Dr.Web Security Control Center configuration file parameters:

○ `<version value="">`

Current version of **Dr.Web Server**.

◆ `<server-name value=""/>`

The name of the **Dr.Web Server**.

Parameter is specified in the following format:

`<Server IP address or DNS name> [: <port>]`



If the **Server** address is not specified, computer name returned by the operating system or the **Server** network address: DNS name, if available, otherwise - IP address are used.

If the port number is not specified, the port from a request is used (e.g., for requests to the **Server** from the **Control Center** or via the **Web API**). Particularly, for the requests from the **Control Center** it is the port specified in the address line for connection of the **Control Center** to the **Server**.

◆ `<document-root value=""/>`

Path to web pages root folder. Default is `value="webmin"`.

◆ `<ds-modules value=""/>`

Path to modules folder. Default is `value="ds-modules"`.

◆ `<threads value=""/>`

Number of parallel requests processed by the **web server**. This parameter affects server performance. It is not recommended to change this parameter without need.

◆ `<io-threads value=""/>`

Number of threads serving data transmitted in network. This parameter affects **Server** performance. It is not recommended to change this parameter without need.

◆ `<compression value="" max-size="" min-size=""/>`

Traffic compression settings for data transmission over a communication channel with the **web server** via HTTP/HTTPS.

Attributes description:

Attribute	Description	Default
value	Data compression level from 1 to 9, where the 1 is minimal level and the 9 is maximal compression level.	9
max-size	Maximal size of HTTP responses which will be compressed. Specify the 0 value to disable limitation on maximal size of HTTP responses to be compressed.	51200 KB
min-size	Minimal size of HTTP responses which will be compressed. Specify the 0 value to disable limitation on minimal size of HTTP responses to be compressed.	32 bytes

◆ `<keep-alive timeout="" send-rate="" receive-rate=""/>`

Keep HTTP session active. Allows to establish permanent connection for requests via the HTTP v. 1.1.

Attributes description:

Attribute	Description	Default
timeout	HTTP session timeout. For persistent connections, Server releases the connection, if there are no requests received from a client during specific time slot.	15 sec.
send-rate	Minimal acceptable data send rate. If outgoing network speed is lower than this value, connection will be rejected. Specify 0 to ignore this limit.	1024 Bps
receive-rate	Minimal acceptable data receive rate. If incoming network speed is lower than this value, connection will be rejected. Specify 0 to ignore this limit.	1024 Bps

◆ `<buffers-size send="" receive=""/>`

Configuration of buffers sizes for sending and receiving data.

Attributes description:

Attribute	Description	Default
send	Size of buffers used when sending data. This parameter affects server performance. It is not recommended to change this parameter without need.	8192 bytes



Attribute	Description	Default
receive	Size of buffers used when receiving data. This parameter affects server performance. It is not recommended to change this parameter without need.	2048 bytes

◆ `<max-request-length value=""/>`

Maximum allowed size of HTTP request in KB.

◆ `<reverse-resolve enabled="no"/>`

Replace IP address with DNS names of computers in the **Server** log file. Allowed values of **enabled**: yes Or no.

◆ `<script-errors-to-browser enabled="no"/>`

Show script errors in browser (error 500). This parameter is used by technical support and developers. It is not recommended to change this parameter without need.

◆ `<trace-scripts enabled=""/>`

Enable scripts tracing. This parameter is used by technical support and developers. It is not recommended to change this parameter without need. Allowed values of **enabled**: yes Or no.

◆ `<profile-scripts enabled="no" stack="no"/>`

Profiling configuration. Performance is measuring - execution time of functions and scripts of the **web server**. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.

Attributes description:

Attribute	Allowed values	Description
enabled	<ul style="list-style-type: none"> yes - enable profiling, no - disable profiling. 	Scripts profiling mode.
stack	<ul style="list-style-type: none"> yes - log data, no - do not log data. 	Logging mode of information on profiling (function parameters and returned values) into the Server log.

◆ `<abort-scripts enabled=""/>`

Allow aborting of scripts execution if the connection was aborted by client. This parameter is used by technical support and developers. It is not recommended to change this parameter without need. Allowed values of **enabled**: yes Or no.

◆ `<search-localized-index enabled=""/>`

Use localized versions of pages. If the flag is set, server searches for localized version of specified page according to the language priority which is set in the `Accept-Language` field of client header. Allowed values of **enabled**: yes Or no.

◆ `<default-lang value=""/>`

Language of documents returned by the **web server** in the absence of the `Accept-Language` header in the HTTP request. The **value** attribute is the ISO language code. Default is `ru`.

◆ `<ssl certificate="" private-key="" keep-alive=""/>`

SSL certificate settings.

Attributes description:

Attribute	Description	Allowed values	Default
certificate	Path to SSL certificate file.	-	certificate.pem
private-key	Path to SSL private key file.	-	private-key.pem



Attribute	Description	Allowed values	Default
keep-alive	Use keep-alive SSL connection. Older browsers may not work properly with regular SSL connections. Disable this parameter, if you have problems with SSL protocol.	<ul style="list-style-type: none"> yes, no. 	yes

◆ <listen>

Configure parameters to listen for network connections.

The <listen /> element contains the following child elements:

- <insecure />

The list of interfaces to listen for accepting connections via the HTTP protocol for unsecured connections. Default port is 9080.

The <insecure /> element contains one or several <endpoint address="" /> child elements to specify allowed addresses in the IPv4 or IPv6 format. In the address attribute, network addresses are specified in the following format: <Protocol>://<IP address>.

- <secure />

The list of interfaces to listen for accepting connections via the HTTPS protocol for secured connections. Default port is 9081.

The <secure /> element contains one or several <endpoint address="" /> child elements to specify allowed addresses in the IPv4 or IPv6 format. In the address attribute, network addresses are specified in the following format: <Protocol>://<IP address>.

◆ <access>

Access control lists. Allow to configure limitations on network addresses to listen for accepting incoming HTTP and HTTPS requests by the **web server**.

The <access /> element contains the following child elements, which configuring limitations for corresponding connection types:

- <secure priority="">

The list of interfaces to listen for accepting secured connections via the HTTPS protocol. Default port is 9081.

Attributes description:

Attribute	Allowed values	Description	Default
priority	allow	Allowance priority for HTTPS - addresses not included in any of the lists (or included into both), are allowed.	deny
	deny	Denial priority for HTTPS - addresses not included in any of the lists (or included into both), are denied.	

The <secure /> element contains one or several following child elements: <allow address="" /> and <deny address="" />.

Elements description:

Element	Description	Default value of address attribute
allow	Addresses which are allowed to access via the HTTPS protocol for secured connections.	tcp://127.0.0.1
deny	Addresses which are denied to access via the HTTPS protocol for secured connections.	-

- <insecure priority="">

The list of interfaces to listen for accepting unsecured connections via the HTTP protocol. Default port is 9080.



Attributes description:

Attribute	Allowed values	Description	Default
priority	allow	Allowance priority for HTTP - addresses not included in any of the lists (or included into both), are allowed.	deny
	deny	Denial priority for HTTP - addresses not included in any of the lists (or included into both), are denied.	

The `<insecure />` element contains one or several following child elements: `<allow address="" />` and `<deny address="" />`.

Elements description:

Element	Description	Default value of address attribute
allow	Addresses which are allowed to access via the HTTP protocol for unsecured connections.	tcp://127.0.0.1
deny	Addresses which are denied to access via the HTTP protocol for unsecured connections.	-

G3. Download.conf Configuration File

The download.conf file purposes:

1. During creating and operating of **Dr.Web Servers** cluster system, the file allows to distribute the load between the **Servers** of a clusters when connecting a large number of new stations.
2. If a custom port is used at **Dr.Web Server**, the file allows to specify this port during generating installation file of the **Agent**.

The `download.conf` file is used during generating the installation file for a new station of the anti-virus network. Parameters of this file allows to specify address of the **Server** and the port, which are used to connect the **Agent** Installer to the **Server**, in the following format:

```
download = { server = '<Server_Address>'; port = <port_number> }
```

where:

- ◆ `<Server_Address>` - IP address or DNS name of the **Server**.

During generating of the **Agent** installation file, the **Server** address is taken from the `download.conf` file first. If the **Server** address is not specified in the `download.conf` file, when value of the `ServerName` parameter from the `webmin.conf` file is taken. Otherwise, the name of the computer, returned by an operating system is used.

- ◆ `<port_number>` - port to connect the **Agent** Installer to the **Server**.

If the port is not specified in the `download.conf` file, 2193 port is used by default (sets in the **Administration** → **Dr.Web Server configuration** → **Transport** tab in the **Control Center**).

By default, the `download` parameter is disabled in the `download.conf` file. To use the `download.conf` file, uncomment this parameter by deleting the `--` in the start of the line, and specify corresponding values of an address and a port of the **Server**.



G4. Proxy Server Configuration File

The `drwcsd-proxy.xml` configuration file of the **Proxy server** is presented in the XML format and located in:

- ◆ For Windows OS: **Proxy server** installation folder.
- ◆ For UNIX system-based OS: `etc` subfolder of the **Proxy server** installation folder or in the current user's work directory.

The `<listen />` element

The `<drwcsd-proxy />` root element contains one or several obligatory `<listen />` elements which define basic settings of the **Proxy Server** for receiving connections. The `<listen />` element contains one obligatory attribute `spec`, attributes of which define an interface to "listen" incoming client connections and whether the `discovery` mode is enabled on this interface. The `spec` attribute contains following properties:

- ◆ `protocol` - type of the protocol for receiving incoming connections. Address which the **Proxy server** listens is set as an attribute.
- ◆ `port` - port which the **Proxy server** listens.
- ◆ `imitation mode` - the mode of **Server** imitation. Allows detection of the **Proxy server** as **Dr.Web Server** by the **Network scanner**.
- ◆ `multicast mode` - network "listening" mode for receiving broadcast requests by the **Proxy server**.
- ◆ `multicast group` - multicast group where the **Proxy server** is located.

Properties values of the `spec` attribute and their parameters are specified in the table G-1.

Table G-1. Properties of the `spec` element

Property	Obligatory	Allowed values	Parameters of possible values	
			Allowed	Default
<code>protocol</code>	yes	<code>ip</code> <code>unix</code>		<code>0.0.0.0</code> -
<code>port</code>	no	<code>port</code>		2193
<code>imitation mode</code>	no	<code>discovery</code>	<code>yes</code> , <code>no</code>	<code>no</code>
<code>multicast mode</code>	no	<code>multicast</code>	<code>yes</code> , <code>no</code>	<code>no</code>
<code>multicast group</code>	no	<code>multicast-group</code>		<code>231.0.0.1</code> <code>[ff18::231.0.0.1]</code>

The `spec` attribute contains one obligatory `protocol` property and three non-obligatory properties, which are: `port`, `imitation mode` and `multicast`. Depending on value of the `protocol` property, the list of non-obligatory properties in the `spec` attribute may vary.

The G-2 table contains the list of non-obligatory properties, which can be set (+) or can not be set (-) in the `spec` attribute, depending on value of the `protocol` parameter.

Table G-2. Presence of non-obligatory properties in dependence of the value of `protocol` parameter

Protocol	Attribute presence			
	<code>port</code>	<code>discovery</code>	<code>multicast</code>	<code>multicast-group</code>
<code>ip</code>	+	+	+	+



Protocol	Attribute presence			
	port	discovery	multicast	multicast-group
unix	+	-	-	-



The **discovery** mode must be enabled directly in any case even if the **multicast** mode is already enabled.

The `<compression />` element defines traffic compression parameters:

- ◆ If the `<compression />` element is a child of the `<forward />` element, it defines compression parameters for the **Server - Proxy server** channel.
- ◆ If the `<compression />` element is a child of the `<listen />` element, it defines compression parameters for the client - **Proxy server** channel.

Table G-3. Attributes of the `<compression />` element

Attribute	Allowed values	Description	Default
mode	yes	compression enabled	possible
	no	compression disabled	
	possible	compression possible	
level	integer from 1 to 9	compression level. Only for the client - Proxy server channel	8

The `<forward />` element

Redirection of incoming connections is adjusted via the `<forward />` element which is a child element of `<listen />`. The `<forward />` element contains one or more obligatory `to` attributes those values define addresses of **Dr.Web Servers** where the connection should be redirected. An address of **Dr.Web Server** is specified according to the [The Specification of Network Addresses](#), in particular, in the following format: `tcp/<DNS_name>:<port>`.

The `<forward />` element is obligatory. Each `<listen />` element can contain several `<forward />` elements.

The forwarding algorithm for the list of **Dr.Web Servers**

1. **Proxy server** loads to RAM the list of **Dr.Web Servers** from the `drwcsd-proxy.xml` configuration file.
2. **Dr.Web Agent** connects to the **Proxy server**.
3. **Proxy server** forwards **Dr.Web Agent** to the first **Server** from **Dr.Web Servers** list loaded in the RAM.
4. **Proxy server** rotate the list in the RAM and moves **Dr.Web Server** from the first position to the end of list.



Proxy Server does not save changed order of **Servers** to its configuration file. After restart of **Proxy server**, the list of **Dr.Web Servers** is loaded to the RAM in original version, which is stored in the configuration file.

5. When the next **Agent** connects to the **Proxy server**, procedure is repeated from the step 2.
6. If **Dr.Web Server** disconnects from the anti-virus network (e.g., gets offline or denies of service), the **Agent** connects to the **Proxy server** repeatedly and procedure is repeated from the step 2.



The <cache /> element

The <drwcsd-proxy /> root element may contain non-obligatory <cache /> element which defines settings of **Proxy server** repository cache.

Table G-4. Attributes of the <cache /> element

Attribute	Allowed values	Description	Default
enabled	yes	caching enabled	yes
	no	caching disabled	

Table G-5. Elements <cache />

Element	Attribute	Allowed values	Default	Description
<repo-root />	-	-	temporary folder of OS user	path to the Proxy server cache folder
<maximum-revision-queue />	size	positive integer	3	number of stored revisions
<clean-interval />	value	positive integer	60	time slot between purging of old revisions in minutes
<unload-interval />	value	positive integer	10	time slot between unloads of unused files from the memory in minutes
<repo-check />	mode	idle/sync	idle	check of cache integrity either at start (may take time) or in background

The <core-dump /> element

The <drwcsd-proxy /> root element may contain the <core-dump /> element in which you can specify collecting mode and number of memory dumps in case of SEH exception occurs.



Memory dumps setup is available for Windows OS only.

To collect memory dump, OS must contain the dbghelp.dll library.

Dump is written to the following folder: %All Users\Application Data%\Doctor Web\drwcsd-proxy-dump\

Table G-6. Attributes of the <core-dump /> element

Attribute	Allowed values	Description	Default
enabled	yes	dumps collecting enabled	yes
	no	dumps collecting disabled	
maximum	positive integer	maximal dumps number. The oldest are deleted	10

Example of drwcsd-proxy.xml configuration file

```
<?xml version="1.0"?>
<drwcsd-proxy>
```



```
<!-- property: ip, unix: define protocol family and address of adapter -->
<!-- property: port: define port to listen on. Default 2193 -->
<!-- property: name: define discovery name. Default drwcs -->
<!-- property: discovery: define should proxy run discovery server too (yes/no). Default no
-->
<!-- property: multicast: define should proxy enter to multicast group (yes/no). Default no
-->
<!-- property: multicast-group: define multicast group address to be entered. Default
231.0.0.1 and ff18::231.0.0.1 -->

<!-- For example -->
<!-- Listen on IN_ADDR_ANY port 2193, run discovery on 231.0.0.1 -->

<listen spec="ip(), discovery(yes), multicast(yes)">
  <forward to="tcp/server1.isp.net:2193">
    <compression mode="no" /> <!-- Compression between proxy and Server -->
  </forward>
  <compression mode="possible" level="4" /> <!-- Compression between proxy and client -->
</listen>

<!-- Listen on ipv6 IN6_ADDR_ANY, port 2194, run discovery on ff18::231.0.0.2 -->
<listen spec="ip([fc01::1]), port(2194), discovery(yes), multicast(yes), multicast-
group([ff18::231.0.0.2])">
  <forward to="tcp/server1.isp.net:2193"/>
  <forward to="tcp/server2.isp.net:2193"/>
</listen>

<!-- Listen on unix -->
<listen spec="unix(/tmp/drwcsd-proxy.sock)">
  <forward to="tcp/server1.isp.net:2193"/>
  <forward to="tcp/server2.isp.net:2193"/>
</listen>

<cache enabled="yes">
  <repo-root>C:\var</repo-root>
  <maximum-revision-queue size="3" />
  <clean-interval value="60" />
  <unload-interval value="10" />
  <repo-check mode="idle" />
</cache>

<core-dump enabled="yes" maximum="7" />
</drwcsd-proxy>
```



Appendix H. Command Line Parameters of the Programs Included in Dr.Web Enterprise Security Suite

H1. Introduction

Command line parameters have a higher priority than the default settings, or other constant settings (set in the **Server** configuration file, Windows OS registry, etc.). In some cases, the parameters specified at launch also predetermine the constant parameters. Such cases are described below.

When describing the syntax of parameters of separate programs optional parts are enclosed in brackets [...].



Features described below in the H1 section, do not applied to the **Agent** network installer.

Some command line parameters have a form of a switch – they begin with a hyphen. Such parameters are also called switches, or options.

Many switches can be expressed in various equivalent forms. Thus, the switches which imply a logical value (*yes/no*, *disable/enable*) have a negative variant, for example, the `-admin-rights` switch has a pair `-no-admin-rights` with the opposite meaning. They can also be specified with an explicit value, for example, `-admin-rights=yes` and `-admin-rights=no`.



The synonyms of *yes* are *on*, *true*, *OK*. The synonyms of *no* are *off*, *false*.

If a switch value contains spaces or tabs, the whole parameter should be put in quotation marks, for example:

```
"-home=c:\Program Files\DrWeb Server"
```



The names of switches can be abbreviated (by omitting the last letters), unless the abbreviated name is to coincide with the beginning of any other switch.

H2. Network Installer

The start instruction format

```
drwinst.exe [<switches>]
```

Switches



Command line switches are valid for launching all types of **Agent** installation files.

Switches to launch the **Agent** network installer are specified in the following format: `/<switch><parameter>`.

All parameters values are specified after the space. For example:

```
/silent yes
```



If a switch value contains spaces, tabs or the / symbol, the whole parameter should be put in quotation marks. For example:

```
/pubkey "C:\my folder\drwcsd.pub"
```

Allowed switches

- ◆ /compression <mode> – compression mode of the traffic with the **Server**. The <mode> parameter may take one of the following values:
 - yes – use compression.
 - no – do not use compression.
 - possible – compression is possible. The final decision is defined depending on settings on the **Server** side.

If the switch is not set, the possible value is used by default.

- ◆ /encryption <mode> – encryption mode of the traffic with the **Server**. The <mode> parameter may take one of the following values:
 - yes – use encryption.
 - no – do not use encryption.
 - possible – encryption is possible. The final decision is defined depending on settings on the **Server** side.

If the switch is not set, the possible value is used by default.

- ◆ /excludeFeatures <components> – the list of components, which must be excluded from installation on the station. To set several components, use the "," sign as a divider. Available components:
 - scanner – **Dr.Web Scanner**,
 - spider-mail – **SpIDer Mail**,
 - spider-g3 – **SpIDer Guard**,
 - outlook-plugin – **Dr.Web for Microsoft Outlook**,
 - firewall – **Dr.Web Firewall**,
 - spider-gate – **SpIDer Gate**,
 - parental-control – **Office Control**,
 - antispam-outlook – **Dr.Web Anti-spam** for **Dr.Web for Microsoft Outlook** component.
 - antispam-spidermail – **Dr.Web Anti-spam** for **SpIDer Mail** component.

Components that are not set directly, save their default installation status.

- ◆ /id <station_id> – identifier of a station on which the **Agent** will be installed.

The switch is specifying with the /pwd switch for automatic authorization on the **Server**. If authorization parameters are not set, authorization decision is defined on the **Server** side.
- ◆ /includeFeatures <components> – the list of components, which must be installed on the station. To set several components, use the "," sign as a divider. Available components:
 - scanner – **Dr.Web Scanner**,
 - spider-mail – **SpIDer Mail**,
 - spider-g3 – **SpIDer Guard**,
 - outlook-plugin – **Dr.Web for Microsoft Outlook**,
 - firewall – **Dr.Web Firewall**,
 - spider-gate – **SpIDer Gate**,
 - parental-control – **Office Control**,



- `antispam-outlook` – **Dr.Web Anti-spam** for **Dr.Web for Microsoft Outlook** component.
- `antispam-spidermail` – **Dr.Web Anti-spam** for **SpIDer Mail** component.

Components that are not set directly, save their default installation status.

- ◆ `/installdir <folder>` – installation folder.

If the switch is not set, default installation folder is the "Program Files\DrWeb" folder on the system drive.

- ◆ `/installtimeout <time>` – waiting limit of reply from a station during the remote installation launched in the **Control Center**. Defined in seconds.

If the switch is not set, 300 seconds are used by default.

- ◆ `/instMode <mode>` – installer launch mode. The `<mode>` parameter may take the following value:
 - `remove` – remove the installed product.

If the switch is not set, by default installer automatically defines the launch mode.

- ◆ `/lang <language_code>` – installer language. Use the ISO-639-1 format to specify the language code.

If the switch is not set, the system language is used by default.

- ◆ `/pubkey` – full path to the **Server** public key file.

If the public key is not set, after the launch of the local installation, installer automatically uses the `drwcsd.pub` public key from own launch folder. If the public key file is located in the folder other than the installer launch folder, you must manually specify the full path to the public key file.

If you launch the installation package generated in the **Control Center**, the public key is included into the installation package and additional specifying of the public key file in the command line switches is not required.

- ◆ `/pwd <password>` – the **Agent** password to access the **Server**.

The switch is specifying with the `/id` switch for automatic authorization on the **Server**. If authorization parameters are not set, authorization decision is defined on the **Server** side.

- ◆ `/regagent <mode>` – defines whether the **Agent** will be registered in the list of installed programs. The `<mode>` parameter may take one of the following values:

- `yes` – register the **Agent** in the list of installed programs.
- `no` – do not register the **Agent** in the list of installed programs.

If the switch is not set, the `no` value is used by default.

- ◆ `/retry <number>` – number of attempts to locate the **Server** by sending multicast requests. If the **Server** has not responded after the specified attempts number is reached, it is assumed what the **Server** is not found.

If the switch is not set, 3 attempts to find the **Server** is performed.

- ◆ `/server [<protocol/>] <server_address>[:<port>]` – the **Server** address from which the **Agent** installation will be performed and to which the **Agent** connects after the installation.

If the switch is not set, by default the **Server** is searched by sending multicast requests.

- ◆ `/silent <mode>` – defines whether the installer will be run in the background mode. The `<mode>` parameter may take one of the following values:

- `yes` – launch the installer in the background mode.
- `no` – launch the installer in the graphical mode.



If the switch is not set, by default the **Agent** installation performs in the graphical mode of the installer (see the **Installation Manual**, p. [Installing Dr.Web Agent via the Installer](#)).

- ◆ /timeout <time> – waiting limit of each reply when searching the **Server**. Defined in seconds. Receiving of response messages continues while the response time is less than the timeout value.

If the switch is not set, 3 seconds are used by default.

H3. Dr.Web Agent

The start instruction format

```
dwservice.exe [<switches>]
```

Switches

Each switch may be set in one of the following formats (formats are equivalent):

```
-<short_switch>[ <argument>]
```

or

```
--<long_switch> [=<argument>]
```

Switches may be used simultaneously including short and long versions.



If an argument contains spaces, it must be enclosed in quotes.

All switches can be executed not dependently on permissions granted for the station on the **Server**. I.e. even if permissions to change the **Agent** settings are denied on the **Server**, you can change these settings via the command line switches.

Allowed switches

- ◆ Show help:
 - -?
 - --help
- ◆ Change address of the **Server** to which the **Agent** connects:
 - -e <Server>
 - --esserver=<Server>

To set several **Servers** at a time, you must repeat via the space character the -e switch for each **Server** address, e.g.:

```
dwservice -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
```

or

```
dwservice --esserver=10.3.1.1:123 --esserver=10.3.1.2:123 --esserver=10.10.1.1:123
```

- ◆ Add the public encryption key:
 - -p <key>
 - --addpubkey=<key>



Public key specified as an argument is copied to the **Agent** folder, is renamed to `drwcsd.pub` (if the name differs) and reread by the service. At this, previous public key file, if presented, is renamed to `drwcsd.pub.old`.

All public keys which were used previously (including keys transmitted from the **Server** and stored in the registry) are remained and can be used if necessary.

◆ Change the **Agent** log level of detail:

- `-l <level>`
- `--loglevel=<level>`

Allowed values of log details level: `err, wrn, inf, dbg`.

H4. Dr.Web Server

There are several variants as how to launch the **Server**. These variants will be described separately.

Commands described in p. [H3.1](#) – [H3.5](#) are crossplatform and enable using in both Windows OS and UNIX system-based OS, unless it is specified otherwise.

H4.1. Managing Dr.Web Server

`drwcsd [<switches>]` – set the parameters for the **Server** operation (the switches are described in more detail below).

H4.2. Basic Commands

- ◆ `drwcsd start` – run the **Server**.
- ◆ `drwcsd restart` – restart the **Server** (it is executed as the `stop` and then `start` pair).
- ◆ `drwcsd stop` – stop the **Server**.
- ◆ `drwcsd reconfigure` – reread and reboot the configuration file (it is performed quicker and without starting a new process).
- ◆ `drwcsd verifyakey <key_file_path>` – verify the **Agent** key file (`agent.key`).
- ◆ `drwcsd verifyekey <key_file_path>` – verify the **Server** key file (`enterprise.key`).
- ◆ `drwcsd verifyconfig <config_file_path>` – verify the syntax of the **Server** configuration file (`drwcsd.conf`).
- ◆ `drwcsd stat` – log statistics to a file: CPU time, memory usage, etc. (for UNIX system-based OS - similar to `send_signal WINCH` or `kill SIGWINCH` commands).

H4.3. Database Commands

Database Initialization

`drwcsd [<keys>] initdb <Agent_key> [<DB_script> [<ini_file> [<password>]]]` – database initialization.

- ◆ `<Agent_key>` – path to **Agent** license key file `agent.key` (must be specified).
- ◆ `<DB_script>` – DB initialization script. A special value - (minus) means not to use such script.



- ◆ `<ini_file>` – previously formed file in the `drweb32.ini` format, which will set the initial configuration of **Dr.Web** software components (i.e. for the **Everyone** group). A special value - (minus) means not to use such file.
- ◆ `<password>` – original password of the **Server** administrator (his name is **admin**). By default, it is **root**.



A minus can be omitted, if the next parameters are missing.

Adjusting parameters of database initialization

If embedded database is used, initialization parameters can be set via an external file. The following command is used for this:

```
drwcsd.exe initdbex <response-file>
```

`<response-file>` - file with initialization parameters written line-by-line in the same order as the `initdb` parameters.

File format:

```
<path_to_key_file>  
<path_to_initdb.sql>  
<path_to_drweb32.ini>  
<administrator_password>
```



If using a response file under Windows OS, any symbols are allowed in the administrator password.

Any strings following the necessary parameter in a particular case are optional. If a string consists of only the minus symbol "-", the default value is used (as in `initdb`).

Database Updating

`drwcsd [<switches>] updatedb <script>` – perform any action with the database (for example, update to a new version) by executing SQL instructors from the `<script>` file.

Database Upgrading

`drwcsd upgradedb <folder>` – run the **Server** to update the structure of the database at a version upgrade (see the `update-db` folder).

Database Export

a) `drwcsd exportdb <file>` – export the database to the specified file.

Example for Windows OS:

```
C:\Program Files\DrWeb Server\bin\drwcsd.exe -home="C:\Program Files\DrWeb  
Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb  
"C:\Program Files\DrWeb Server\esbase.es"
```



Under **UNIX** system-based OS, the action is performed on behalf of the `drwcs:drwcs` user to the `$DRWCS_VAR` directory (except **FreeBSD** OS, which by default saves the file to the directory from which the script was run; if the path is specified explicitly, then the directory should have the write access for the `<user>:<group>` that had been created at installation, by default it is `drwcs:drwcs`).

- b) `drwcsd xmlexportdb <xml_file>` – export the database to the specified xml file.

If you specify the `gz` file extension, when during the export, database file will be packed into the gzip archive.

If you do not specify any extension or specify an extension other than `gz`, when export file will not be archived.

Example for Windows OS:

- To export the database into the xml file with no compression:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" "-home=C:\Program Files\DrWeb Server" "-bin-root=C:\Program Files\DrWeb Server" "-var-root=C:\Program Files\DrWeb Server\var" -verbosity=ALL -rotate=10,10m -log=export.log xmlexportdb database.db
```

- To export the database into the xml file compressed to an archive:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" "-home=C:\Program Files\DrWeb Server" "-bin-root=C:\Program Files\DrWeb Server" "-var-root=C:\Program Files\DrWeb Server\var" -verbosity=ALL -rotate=10,10m -log=export.log xmlexportdb database.gz
```

Example for UNIX system-based OS:

- To export the database into the xml file with no compression:

```
/etc/init.d/drwcsd xmlexportdb /test/database.db
```

- To export the database into the xml file compressed to an archive:

```
/etc/init.d/drwcsd xmlexportdb /es/database.gz
```

Database Import

- a) `drwcsd importdb <file>` – import the database from the specified file (the previous content of the database is deleted).
- b) `drwcsd xmlimportdb <xml_file>` – import the database from the specified xml file.
- c) `upimportdb <file>` – import the database exported from the **Server** of previous version.
- d) `upxmlimportdb <xml_file>` – import the database exported in xml from the **Server** of previous version.

Database Verification

`drwcsd verifydb` – run the **Server** to check the database. Upon completion, the **Server** saves the verification results in the log file (`drwcsd.log` by default).

Database speed up

`drwcsd [switches] speedupdb` – execute the `VACUUM`, `CLUSTER`, `ANALYZE` commands to speed up the DB operation.



H4.4. Repository Commands

- ◆ `drwcsd syncrepository` – synchronize the repository with the **GUS**. Stop the **Server** before initiating this instruction!
- ◆ `drwcsd rerepository` – reread the repository from the drive.

H4.5. Backup of Dr.Web Server Critical Data

The following command creates backup copies of critical **Server** data (database contents, the license key file, private encryption key, **Server** configuration file, and **Dr.Web Security Control Center** configuration file):

`drwcsd -home=<path> backup [<directory> [<quantity>]]` – copy critical **Server** data to the specified folder. `-home` sets the **Server** installation catalog. `<quantity>` is the number of copies of each file.

Example for Windows OS:

```
C:\Program Files\DrWeb Server\bin>drwcsd -home="C:\Program Files\DrWeb Server"
backup C:\a
```

The copies are stored in the `.gz` format ununpackable with `gzip` and other archivers. After unpacking all the files, except for the database contents, are ready to use. To restore the data, the database contents can be imported from the backup to another database of the **Server** by means of the `importdb` switch (see p. [Restoring the Database of Dr.Web Enterprise Security Suite](#)).

Starting from the **4.32** version, **Dr.Web Enterprise Security Suite** regularly stores backups of critical information to `\var\Backup` of the **Server** installation catalog. For that purpose a daily task is included to the **Server** schedule, which performs this function. If such task is missing, it is strongly recommended to create it. Particularly there will be no backup critical data task, if the initially installed (and then consequently upgraded) **Server** version is **4.32**.

H4.6. Commands for Windows® OS Only

- ◆ `drwcsd [<switches>] install` – install the **Server** service in the system.
- ◆ `drwcsd uninstall` – uninstall the **Server** service from a system.
- ◆ `drwcsd kill` – perform emergency shutdown of the **Server** service (if normal termination failed). This instruction should not be used without extreme necessity.
- ◆ `drwcsd silent` – disable messages from the **Server**. Used in command files to disable **Server** interactivity.



H4.7. Commands for UNIX® System-Based OS Only

- ◆ `drwcsd config` – similar to `reconfigure` or `kill SIGHUP` commands – restart the **Server**.
- ◆ `drwcsd dumpimportdb` – write to the **Server** log file detailed information on import to embedded or external database.
- ◆ `drwcsd interactive` – run the **Server**, but do not direct the control to the process.
- ◆ `drwcsd newkey` – generate a new encryption keys (`drwcsd.pri` and `drwcsd.pub`).
- ◆ `drwcsd readtempl` – reread notification templates from the drive.
- ◆ `drwcsd readrepo` – reread repository from the drive.
- ◆ `drwcsd selfcert` – generate a new SSL certificate (`certificate.pem`) and RSA private key (`private-key.pem`).
- ◆ `drwcsd shell <file_name>` – run the binary file.
- ◆ `drwcsd showpath` – show all program paths, registered in the system.
- ◆ `drwcsd status` – show the current status of the **Server** (running, stopped).

H4.8. The Description of Switches

Crossplatform Switches

- ◆ `-activation-key=<license_key>` – **Server** license key. By default, it is the `enterprise.key` file located in the `etc` subfolder of the root folder.
- ◆ `-bin-root=<folder_for_executables>` – the path to executable files. By default, it is the `bin` subfolder of the root folder.
- ◆ `-conf=<configuration_file>` – name and location of the **Server** configuration file. By default, it is the `drwcsd.conf` file in the `etc` subfolder of the root folder.
- ◆ `-daemon` – for Windows platforms it means to launch as a service; for UNIX platforms - "daemonization of the process" (to go to the root folder, disconnect from the terminal and operate in the background).
- ◆ `-db-verify=on` – check database integrity at **Server** start. This is the default value. It is not recommended to run with an explicit opposite value, except if run immediately after the database is checked by the `drwcsd verifydb` instruction, see above.
- ◆ `-help` – displays help. Similar to the programs described above.
- ◆ `-hooks` – to permit the **Server** to perform user extension scripts located in the:
 - for Windows OS: `var\extensions`
 - for FreeBSD OS: `/var/drwcs/extensions`
 - for Linux OS and Solaris OS: `/var/opt/drwcs/extensions`subcatalog of the **Server** installation catalog. The scripts are meant for automation of the administrator work enabling quicker performance of certain tasks. All scripts are disabled by default.
- ◆ `-home=<root>` – **Server** installation folder (root folder). The structure of this folder is described in **Installation Manual**, p. [Installing Dr.Web Server for Windows® OS](#). By default, it is the current folder at start.
- ◆ `-log=<log>` – **Server** log filename. A minus can be used instead of the filename (for **Servers** under UNIX OS only), which instructs standard output of the log. By default: for Windows platforms it is `drwcsd.log` in the folder specified by the `-var-root` switch, for UNIX platforms it is set by the `-syslog=user` switch (read below).
- ◆ `-private-key=<private_key>` – private **Server** key. By default, it is `drwcsd.pri` in the `etc` subfolder of the root folder.
- ◆ `-rotate=<N><f>, <M><u>` – **Server** log rotation mode, where:



Parameter	Description
<N>	Total number of log files (including current and archive).
<f>	Log files storing format, possible values: <ul style="list-style-type: none">◆ z (gzip) – compress files, used by default,◆ p (plain) – do not compress files.
<M>	Log file size or rotation time, depending on the <u> value;
<u>	unit measure, possible values: <ul style="list-style-type: none">◆ to set rotation by log file size:<ul style="list-style-type: none">• k - Kb,• m - Mb,• g - Gb.◆ to set rotation by time:<ul style="list-style-type: none">• H - hours,• D - days,• W - weeks.



If rotation by time is set, synchronization performs independently on command launch time: the H value means synchronization with the beginning of an hour, D - with beginning of a day, W - with beginning of a week (00:00 on Monday) according to the multiplicity specified in the <u> parameter.

Initial reference point - January 01, year 01 AD, UTC+0.

By default, it is 10,10m, which means storing of 10 files 10 megabytes each, use compression. Alternatively you can use the none format (-rotate=none), which means "do not use rotation, always write to the same file of unlimited size".

In the rotation mode, log file names are generated as follows: file.<N>.log or file.<N>.log.gz, where <N> - sequence number: 1, 2, etc.

For example, the log file name is set to file.log (see the -log switch above), then

- file.log – current log file,
 - file.1.log – previous log file,
 - file.2.log and so on – the greater the number, the older the version of the log.
- ◆ -trace – to log in detail the location of error origin.
 - ◆ -var-root=<folder_for_modified> – path to a folder to which the **Server** has a write access and which is designed to store modified files (for example, logs and the repository files). By default, it is the var subfolder of the root folder.
 - ◆ -verbosity=<details_level> – log level of detail. WARNING is by default. Allowed values are: ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. The ALL and DEBUG3 values are synonyms (see also [Appendix K. Log Files Format](#)).



This key defines the log level of detail set by the subsequent -log key (read above). One instruction can contain several switches of this type.

The -verbosity and -log switches are position-relative.

In case of using these keys simultaneously, the -verbosity switch must be set before the -log switch: the -verbosity switch redefines detail level of logs, that reside in folder, specified in the following switch.



Switches for Windows OS Only

- ◆ `-minimized` – (if run not as a service, but in the interactive mode) – minimize a window.
- ◆ `-screen-size=<size>` – (if run not as a service, but in the interactive mode) – log size in lines displayed in the **Server** screen, the default value is 1000.

Switches for UNIX system-based OS Only

- ◆ `-etc=<path>` – path to the `etc (<var>/etc)` directory.
- ◆ `-pid=<file>` – a file to which the **Server** writes the identifier of its process.
- ◆ `-syslog=<mode>` – instructs logging to the system log. Possible modes: `auth`, `cron`, `daemon`, `kern`, `lpr`, `mail`, `news`, `syslog`, `user`, `uucp`, `local0` – `local7` and for some platforms – `ftp`, `authpriv`.



The `-syslog` and `-log` keys work together. I.e., if you start the **Server** with the `-syslog` key (e.g., `service drwcsd start -syslog=user`), the **Server** run with specified value for the `-syslog` key and with default value for the `-log` key.

- ◆ `-user=<user>`, `-group=<group>` – available for UNIX OS only, if run by the root user; it means to change the user or the group of process and to be executed with the permissions of the specified user (or group).

H4.9. Variables for UNIX® System-Based OS Only

To make the administration of the **Server** under UNIX system-based OS easier, administrator is provided with variables which reside in the script file stored in the following folder:

- For Solaris OS and Linux OS: `/etc/init.d/drwcsd`.
- For FreeBSD OS: `/usr/local/etc/rc.d/drwcsd.sh` (symbolic link to the `/usr/local/etc/drweb.com/software/init.d/drwcsd`).

Correspondence between variables and [command switches](#) for the `drwcsd` is described in the Table H-1.

Table H-1.

Switch	Variable	Default parameters
<code>-home</code>	<code>DRWCS_HOME</code>	<ul style="list-style-type: none"> • <code>/usr/local/drwcs</code> - for the FreeBSD OS, • <code>/usr/drwcs</code> - for all other OS.
<code>-var-root</code>	<code>DRWCS_VAR</code>	
<code>-etc</code>	<code>DRWCS_ETC</code>	<code>\$DRWCS_VAR/etc</code>
<code>-rotate</code>	<code>DRWCS_ROT</code>	<code>10,10m</code>
<code>-verbosity</code>	<code>DRWCS_LEV</code>	<code>trace3</code>
<code>-log</code>	<code>DRWCS_LOG</code>	<code>\$DRWCS_VAR/log/drwcsd.log</code>
<code>-conf</code>	<code>DRWCS_CFG</code>	<code>\$DRWCS_ETC/drwcsd.conf</code>
<code>-pid</code>	<code>DRWCS_PID</code>	
<code>-user</code>	<code>DRWCS_USER</code>	
<code>-group</code>	<code>DRWCS_GROUP</code>	
<code>-hooks</code>	<code>DRWCS_HOOKS</code>	
<code>-trace</code>	<code>DRWCS_TRACE</code>	



DRWCS_HOOKS and DRWCS_TRACE variables do not have any parameters. If variables have been defined, corresponding switches will be added during the script execution. If variables have not been defined, switches will not be added.

Other variables are described in the Table H-2.

Table H-2.

Variables	Default parameters	Description
DRWCS_ADDOPT		
DRWCS_CORE	unlimited	The core file maximal size.
DRWCS_FILES	8192	The maximal number of file descriptors, that the Server is able to open.
DRWCS_BIN	\$DRWCS_HOME/bin	The directory to start the <code>drwcsd</code> from.
DRWCS_LIB	\$DRWCS_HOME/lib	The directory with Server libraries.

Default values of parameters will be used, if these variables have not been defined in the `drwcsd` script.



DRWCS_HOME, DRWCS_VAR, DRWCS_ETC, DRWCS_USER, DRWCS_GROUP, DRWCS_HOOKS variables are already defined in the `drwcsd` script file.

If the `${TGT_ES_ETC}/common.conf` file exists, this file will be included to the `drwcsd`, that could redefine some variables, but if they are not exported (using the `export` command), they will not take any effect.

To set variables, do the following:

1. Add variable definition to the `drwcsd` script file.
2. Export this variable using the `export` command (at the same place).
3. When one more process will be run from this script, this process will read values that have been set.

H5. Administrating Utility of the Embedded Database

The following utility of embedded DB management are provided:

- ◆ `drwidbsh` - for the IntDB database,
- ◆ `drwidbsh3` - for the SQLite3 database.

Utilities reside in the following folders:

- ◆ for **Linux** OS and **Solaris** OS: `/opt/drwcs/bin`
- ◆ for **FreeBSD** OS: `/usr/local/drwcs/bin`
- ◆ for **Windows** OS:

`<Server_installation_folder>\bin`

(by default, the **Server** installation folder is: `C:\Program Files\DrWeb Server`).

The start instruction format:

`drwidbsh <path_to_DB_file>`

or



```
drwidbsh3 <path_to_DB_file>
```

The program operates in the text dialog mode; it waits for instructions from a user (the instructions begin with a period).

To receive help on other instructions, type `.help`.

For more information, use reference manuals on the SQL language.

H6. Utility of Generation of Key Pairs and Digital Signatures

The names and location of encryption files in the Server installation directory:

- ◆ `\etc\drwcsd.pri` - private key,
- ◆ `\Installer\drwcsd.pub` - public key.

Variants of the instruction format:

- ◆ `\bin\drwsign check [-public-key=<public>] <file>`
Check the file signature using `<public>` as a public key of a person who signed this file.
- ◆ `\bin\drwsign extract [-private-key=<private>] <public>`
Extract the public key from the private key file of a complex format (version **4.33** and higher).
- ◆ `\bin\drwsign genkey [<private> [<public>]]`
Generate the public-private pair of keys and write them to correspondent files.



The utility version for Windows platforms (in contrast to UNIX versions) does not protect private keys from copying.

- ◆ `\bin\drwsign help [<instruction>]`
Brief help on the program and on the command line format.
- ◆ `\bin\drwsign join432 [-public-key=<public>] [-private-key=<private>] <new_private>`
Combines the public and private keys of the format for version **4.32** into a new format of the private key for version **4.33**.
- ◆ `\bin\drwsign sign [-private-key=<private>] <file>`
Sign the `<file>` file using this private key.

H7. Administration of Dr.Web Server Version for UNIX® OS with the kill Instruction

The version of the **Server** for UNIX OS is administrated by the signals sent to the **Server** processor by the `kill` utility.



Use the `man kill` instruction to receive help on the `kill` utility.

Below are listed the utility signals and the actions performed by them:

- ◆ `SIGWINCH` – log statistics to a file (CPU time, memory usage, etc.),



- ◆ SIGUSR1 – reread the repository from the drive,
- ◆ SIGUSR2 – reread templates from the drive,
- ◆ SIGHUP – restart the **Server**,
- ◆ SIGTERM – shut down the **Server**,
- ◆ SIGQUIT – shut down the **Server**,
- ◆ SIGINT – shut down the **Server**.

Similar actions are performed by the switches of the `drwcsd` instruction for the Windows version of the **Server**, read Appendix [H3.3](#).

H8. Dr.Web Scanner for Windows®

This component of the workstation software has the command line parameters which are described in the **Dr.Web® Agent for Windows** User Manual. The only difference is that when the Scanner is run by the **Agent**, the `/go /st` parameters are sent to the **Server** automatically and without fail.

H9. Proxy Server

To configure some of the **Proxy server** parameters, run with corresponding switches the `drwcsd-proxy` executable file, which resides in:

- ◆ For Windows OS: **Proxy server** installation folder.
- ◆ For UNIX system-based OS: `bin` subfolder of the **Proxy server** installation folder.

The start instruction format:

```
drwcsd-proxy <switches>
```

Possible switches:

- ◆ `--help` – show help message on switches for **Proxy server** setting.
- ◆ `--daemon` – for UNIX system-based OS only: run the **Proxy server** as daemon.
- ◆ `--control <arg>` – for Windows OS only: specify parameters for service configuration.

Allowed parameters:

- `run` – (by default) run the **Proxy server** in a background mode as a Windows OS service.
- `install` – install the **Proxy server**.
- `uninstall` – uninstall the **Proxy server**.
- ◆ `--cfg <path>` – path to the **Proxy server** [configuration file](#).
- ◆ `--pool-size <N>` – pool size for clients connections. Default is 2.
- ◆ `--trace` – enable detailed logging of **Proxy server** calls. Available only if the **Proxy server** supports calls stack tracing.
- ◆ `--use-console-log` – write **Proxy server** log to console.
- ◆ `--use-file-log <file>` – write **Proxy server** log to a file, where the `<file>` is a path to log file.
- ◆ `--rotate=<N><f>, <M><u>` – **Proxy server** log rotation mode, where:

Parameter	Description
<code><N></code>	Total number of log files (including current and archive).
<code><f></code>	Log files storing format, possible values: <ul style="list-style-type: none"> ◆ <code>z</code> (gzip) – compress files, used by default,



Parameter	Description
	◆ p (plain) – do not compress files.
<M>	Log file size or rotation time, depends on the <u> value;
<u>	unit measure, possible values: ◆ to set rotation by log file size: <ul style="list-style-type: none">• k - Kb,• m - Mb,• g - Gb. ◆ to set rotation by time: <ul style="list-style-type: none">• H - hours,• D - days,• W - weeks.



If rotation by time is set, synchronization performs independently on command launch time: the H value means synchronization with the beginning of an hour, D - with beginning of a day, W - with beginning of a week (00:00 on Monday) according to the multiplicity specified in the <u> parameter.

Initial reference point - January 01, year 01 AD, UTC+0.

By default, it is 10, 10m, which means storing of 10 files 10 megabytes each, use compression.

- ◆ --verbosity=<details_level> – log level of detail. TRACE3 is by default. Allowed values are: ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. The ALL and DEBUG3 values are synonyms.



All switches for setting **Proxy server** parameters can be set simultaneously.

Writing log to the file and to the console simultaneously is not supported. Meanwhile:

- ◆ If none of switches is specified, log is written to the console.
- ◆ If both of switches are specified, log is written to the file.

H10. Dr.Web Server Remote Diagnostics Utility

Dr.Web Server remote diagnostics utility allows remotely connect to **Dr.Web Server** for basic controlling and viewing the operation statistics.

Console version of the utility is located in the `bin` folder of the **Server** installation folder.



For connection of the **Server** remote diagnostics utility, you must enable **Dr.Web Server FrontDoor** extension. To do this, in the **Dr.Web Server configuration** section, on the **Modules** tab, set the **Dr.Web Server FrontDoor extension** flag.

For connection of the **Server** remote diagnostics utility, administrator that connects via the utility, must have the **Use additional features** permission. Otherwise, access to the **Server** via the remote diagnostics utility will be forbidden.

The **Server** settings to connect **Dr.Web Server** remote diagnostics utility are given in the **Administrator Manual**, p. [Dr.Web Server Remote Access](#).



Utility Console Version

The start instruction format:

```
drwcntl [-?|-h|--help] [+<log_file>] [<server> [<login> [<password>]]]
```

where:

- ◆ `-? -h --help` – show help message on commands for using the utility.
- ◆ `<log_file>` – write all utility actions into the log file by the specified path.
- ◆ `<server>` – address of the **Server**, to which the utility connects in the following format: `[(tcp|ssl)://]<IP address or DNS name>[:<port>]`.
- ◆ `<login>` – login of the **Server** administrator.
- ◆ `<password>` – administrative password to access the **Server**.

Possible commands:

- ◆ `cache <operation>` – operations with file cache. To request the certain operation, use the following commands:
 - `clear` – clear the file cache,
 - `list` – show all file cache content,
 - `matched <regular expression>` – show file cache content which matches the specified regular expression,
 - `maxfilesize [<size>]` – show/set maximal size of preloaded file objects. When launched without additional parameters, shows the current size. To set the size, specify necessary size in bytes after the command name.
 - `statistics` – show statistics of file cache usage.
- ◆ `calculate <function>` – calculate specified sequence. To request the certain sequence, use the following commands:
 - `hash [<standard>] [<string>]` – calculate hash of specified string. To set the certain standard, use the following commands:
 - `gost` – calculate hash of specified string according to the GHOST standard,
 - `md5` – calculate md5 hash of specified string,
 - `sha` – calculate hash of specified string according to the SHA standard,
 - `sha1` – calculate hash of specified string according to the SHA1 standard,
 - `sha224` – calculate hash of specified string according to the SHA224 standard,
 - `sha256` – calculate hash of specified string according to the SHA256 standard,
 - `sha384` – calculate hash of specified string according to the SHA384 standard,
 - `sha512` – calculate hash of specified string according to the SHA512 standard.
 - `hmac [<standard>] [<string>]` – calculate HMAC of specified string. To set the certain standard, use the following commands:
 - `md5` – calculate the HMAC-MD5 for the specified string,
 - `sha256` – calculate the HMAC-SHA256 for the specified string.
 - `random` – generate random number,
 - `uuid` – calculate unique identifier.
- ◆ `clients <operation>` – get information and manage clients connected to the **Server**. To request the certain function, use the following commands:
 - `addresses [<regular expression>]` – show stations network addresses that match specified regular expression. If the regular expression is not specified, show addresses of all stations.



- `addresses` [*<regular expression>*] – show the number of station IP addresses that match specified regular expression. If the regular expression is not specified, show the number of all stations.
- `chosts` [*<regular expression>*] – show the number of station computer names that match specified regular expression. If the regular expression is not specified, show the number of all stations.
- `cids` [*<regular expression>*] – show the number of station identifiers that match specified regular expression. If the regular expression is not specified, show the number of all stations.
- `cnames` [*<regular expression>*] – show the number of station names that match specified regular expression. If the regular expression is not specified, show the number of all stations.
- `disconnect` [*<regular expression>*] – terminate current active connections with stations whose identifiers match specified regular expression. If the regular expression is not specified, terminate connection with all connected stations.
- `enable` [*<mode>*] – show/set the mode of accepting clients at the **Server**. When launched without additional parameters, shows the current mode. To set the mode, use the following additional commands:
 - `on` – accept all client connections.
 - `off` – reject all client connections.
- `hosts` *<regular expression>* – show station computer names that match specified regular expression.
- `ids` *<regular expression>* – show station identifiers that match specified regular expression.
- `names` *<regular expression>* – show station names that match specified regular expression.
- `online` *<regular expression>* – show online time of the stations whose identifier, name or address match specified regular expression. Online time starts from the moment of last connection of the stations to the **Server**.
- `statistics` *<regular expression>* – show statistics on number of clients that match specified regular expression.
- `traffic` *<regular expression>* – show traffic information of currently connected clients that match specified regular expression.
- ◆ `core` – write the **Server** process dump.
- ◆ `cpu` *<parameter>* – show statistics of the computer CPU usage on which the **Server** is installed. To request the certain parameter, use the following commands:
 - `clear` – delete all accumulated statistic data,
 - `day` – show CPU loading graph for the current day,
 - `disable` – disable monitoring of CPU loading,
 - `enable` – enable monitoring of CPU loading,
 - `hour` – show CPU loading graph for the current hour,
 - `load` – show average CPU loading,
 - `minute` – show CPU loading graph for the passed minute,
 - `rawd` – show numeric statistic on CPU loading for the day,
 - `rawh` – show numeric statistic on CPU loading for the last hour,
 - `rawl` – show numeric statistic on average CPU loading,
 - `rawm` – show numeric statistic on CPU loading for the last minute,
 - `status` – show the monitoring state of CPU loading.
- ◆ `debug` *<parameter>* – debug configuration. To set the certain parameter, use the additional commands. To refine the additional commands list, you can call the help by the `? debug` command.



The `debug signal` command is available for the **Servers** under UNIX system-based OS only.

- ◆ `die` – stop the **Server** and write the **Server** process dump.



The `die` command is available for the **Servers** under UNIX system-based OS only.

- ◆ `dwcp <parameter>` – set/show **Dr.Web Control Protocol** (includes **Server**, **Agent** and **Agent installers protocols**) options. Allowed parameters:
 - `compression <mode>` – set the one of the following traffic compression modes:
 - `on` – compression enabled,
 - `off` – compression disabled,
 - `possible` – compression is possible.
 - `encryption <mode>` – set the one of the following traffic encryption modes:
 - `on` – encryption enabled,
 - `off` – encryption disabled,
 - `possible` – encryption is possible.
 - `show` – show current **Dr.Web Control Protocol** options.
- ◆ `io <parameter>` – show input/output statistics of the **Server** process. To request the certain parameter, use the following command:
 - `clear` – delete all accumulated statistic data,
 - `disable` – disable statistics monitoring,
 - `enable` – enable statistics monitoring,
 - `rawdr` – show numeric statistic on data read for the day,
 - `rawd` – show numeric statistic on data write for the day,
 - `rawh` – show numeric statistic for the last hour,
 - `rawm` – show numeric statistic for the last minute,
 - `rday` – show data read graph for the current day,
 - `rhour` – show data read graph for the last hour,
 - `rminute` – show data read graph for the last minute,
 - `status` – show statistics monitoring state,
 - `wday` – show data write graph for the day,
 - `whour` – show data write graph for the last hour,
 - `wminute` – show data write graph for the last minute.
- ◆ `log <parameter>` – write the string to the **Server** log file or set/view the log verbosity level. Depending on the specified parameters, the following actions are performed:
 - `log <string>` - write the specified string to the **Server** log file with the `NOTICE` verbosity level.
 - `log \s [<level/>]` - set/show the log verbosity level. If the command launched with the `\s` command with no level specified, the current verbosity level is shown. Available values of the log verbosity level: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`.
- ◆ `lua` – execute LUA script.
- ◆ `mallopt <parameter>` – set the parameters of the memory allocation. To set the certain parameter, use the additional commands. To refine the additional commands list, you can call the help by the `? mallopt` command.



The `mallopt` command is available for the **Servers** under Linux system-based OS only.

To get more details on the command parameters features, refer the description of the `mallopt()` function from the `glibc` library. To get the help on this function, you can use the `man mallopt` command.

- ◆ `memory <parameter>` – show statistics of the computer memory usage on which the **Server** is installed. To request the certain parameter, use the following commands:
 - `all` – show all information and statistic data,
 - `heap` – show information on dynamic memory,
 - `malloc` – show statistic on memory allocation,
 - `sizes` – show statistic on allocated memory sizes,
 - `system` – show information on system memory.



The `memory` command is available for the **Servers** under Windows OS, Linux system-based OS and FreeBSD system-based OS only. At this, the following limitations on additional parameters of the `memory` command are active:

- `system` - for the **Servers** under Windows OS, Linux system-based OS only,
- `heap` - for the **Servers** under Windows OS, Linux system-based OS only,
- `malloc` - for the **Servers** under Linux system-based OS and FreeBSD system-based OS only,
- `sizes` - for the **Servers** under Linux system-based OS and FreeBSD system-based OS only.

- ◆ `monitoring <mode>` – set/show monitoring mode of CPU (the `cpu <parameter>` command) and I/O (the `io <parameter>` command) resources usage by the **Server** process. Allowed parameters:
 - `disable` – disable monitoring,
 - `enable` – enable monitoring,
 - `show` – show current mode.
- ◆ `printstat` – write the **Server** operation statistic to the log.
- ◆ `reload` – reload **Dr.Web Server FrontDoor** extension.
- ◆ `repository <parameter>` – repository management. To request the certain function, use the following commands:
 - `all` – show the list of all repository products and the number of all files by products,
 - `clear` – clear cache content not depending on the TTL value of the objects in the cache,
 - `fill` – read all repository files into cache,
 - `keep` – store all repository files currently in the cache forever, not depending on their TTL value,
 - `loaded` – show the list of all repository products and the number of all files by products which are currently in the cache,
 - `reload` – reload repository from disk,
 - `statistics` – show repository updates statistics.
- ◆ `restart` – restart the **Server**.
- ◆ `show <parameter>` – show the information about the system on which the **Server** is installed. To set the certain parameter, use the additional commands. To refine the additional commands list, you can call the help by the `? show` command.



the following limitations on additional parameters of the `show` command are active:

- `memory` - for the **Servers** under Windows OS, Linux system-based OS only,
- `mapping` - for the **Servers** under Windows OS, Linux system-based OS only,



- `limits` - for the **Servers** under UNIX system-based OS only,
 - `processors` - for the **Servers** under Linux system-based OS only.
-

- ◆ `sql` – execute SQL query.
- ◆ `stop` – stop the **Server**.
- ◆ `traffic <parameter>` – show statistic on the **Server** network traffic. To request the certain parameter, use the following commands:
 - `all` – show all the traffic from the **Server** start.
 - `incremental` – show traffic incrementation from the last launch of the `traffic incremental` command.
 - `last` – show traffic incrementation from the last stored point.
 - `store` – create the stored point for the `last` command.
- ◆ `update <parameter>` – get information and manage updates. To request the certain function, use the following commands:
 - `active` – show the list of **Agents** which are currently updating.
 - `agent [<mode>]` – show/set the mode of updating the **Agents** from the **Server**. When launched without additional parameters, shows the current mode. To set the mode, use the following additional commands:
 - `on` – enable **Agents** updates.
 - `off` – disable **Agents** updates.
 - `gus` – launch the repository update from the **GUS** ignoring the **GUS** update state.
 - `http [<mode>]` – show/set the mode of updating the **Server** repository from the **GUS**. When launched without additional parameters, shows the current mode. To set the mode, use the following additional commands:
 - `on` – enable repository updating from the **GUS**.
 - `off` – disable repository updating from the **GUS**.
 - `inactive` – show the list of **Agents** which are not currently updating.
 - `track [<mode>]` – show/set the mode of tracking the **Agents** update. When launched without additional parameters, shows the current mode. To set the mode, use the following additional commands:
 - `on` – enable **Agents** update tracking.
 - `off` – disable **Agents** update tracking. At this, the `update active` command will not show the list of currently updating **Agents**.

H11. Dr.Web Server Installer for UNIX® System-Based OS

The start instruction format

`<package_name>.run [<switches>] [--] [<arguments>]`

where:

- `[--]` – separate optional sign, determines the end of the switches list and separates the switches list and the additional arguments list.
- `[<arguments>]` – additional arguments or embedded scripts. Are not used in the current version of the **Server** installer.

Switches to get help or information on the package:

- `--help` – show the help on switches.



- `--info` – show extended information on the package: the name; destination folder; unpacked size; compression algorithm; compression date; the version of `make` which is used for packing; the command user for packing; the script that will be launched after unpacking; whether the archive content will be copied into the temporary folder or not (if no, nothing shown); whether the destination folder stored or will be deleted after the script execution.
- `--lsm` – show the LSM file with installation package description (or **no LSM** if the file is absent).
- `--list` – show the list of files in the installation package.
- `--check` – check integrity of the installation package.

Switches to run the package:

- `--confirm` – ask before running embedded script.
- `--noexec` – do not run embedded script.
- `--keep` – do not clear target directory after running the embedded script.
- `--noxl1` – do not try to launch the graphical terminal emulation.
- `--nochown` – do not grant permissions for the extracted files to the current user.
- `--target <folder>` – extract the installation package to the specified folder.
- `--tar <argument_1> [<argument_2> ...]` – get access the contents of the installation package through the `tar` command.



Appendix I. Environment Variables Exported by Dr.Web Server

To simplify the setting of the processes run by **Dr.Web Server** on schedule, the data on location of the **Server** catalogs is required. To this effect, the **Server** exports the following variables of started processes into the environment:

- ◆ `DRWCSD_HOME` – path to the root folder (installation folder). The switch value is `-home`, if it was set at **Server** launch; otherwise the current folder at launch.
- ◆ `DRWCSD_EXE` – path to the folder with executable files. The switch value is `-bin-root`, if it was set at **Server** launch; otherwise it is the `bin` subfolder of the root folder.
- ◆ `DRWCSD_VAR` – path to the folder to which the **Server** has a write access and which is designed to store volatile files (for example, logs and repository files). The switchvalue is `-var-root`, if it was set at **Server** launch; otherwise it is the `var` subfolder of the root folder.



Appendix J. Regular Expressions Used in Dr.Web Enterprise Security Suite

Some parameters of **Dr.Web Enterprise Security Suite** are specified in the form of regular expressions of the following types:

- ◆ Regular expressions of Lua language.

Used for configure an automatic membership of anti-virus network stations into user groups.

Detailed description of Lua language regular expressions is available at <http://www.lua.org/manual/5.1/manual.html#5.4.1>.

- ◆ Regular expressions of PCRE program library.

Detailed description of PCRE library syntax is available at <http://www.pcre.org/>.

This appendix contains only a brief description of the most common examples for using regular expressions of PCRE library.

J1. Options Used in PCRE Regular Expressions

Regular expressions are used in the configuration file and in **Dr.Web Security Control Center** when objects to be excluded from scanning in the **Scanner** settings are specified.

Regular expressions are written as follows:

```
qr{EXP}options
```

where `EXP` is the expression itself; `options` stands for the sequence of options (a string of letters), and `qr{}` is literal metacharacters. The whole construction looks as follows:

```
qr{pagefile\.sys}i - Windows NT OS swap file
```

Below goes the description of options and regular expressions. For more details visit <http://www.pcre.org/pcre.txt>.

- ◆ Option 'a' is equivalent to `PCRE_ANCHORED`

If this option is set, the pattern is forced to be "anchored", that is, it is constrained to match only at the first matching point in the string that is being searched (the "subject string"). The same result can also be achieved by appropriate constructs in the pattern itself.

- ◆ Option 'i' is equivalent to `PCRE_CASELESS`

If this option is set, letters in the pattern match both upper and lower case letters. This option can be changed within a pattern by a `(?i)` option setting.

- ◆ Option 'x' is equivalent to `PCRE_EXTENDED`

If this option is set, whitespace data characters in the pattern are totally ignored except when escaped or inside a character class. Whitespaces do not include the VT character (code 11). In addition, characters between an unescaped `#` outside a character class and a newline character inclusively are ignored. This option can be changed in the pattern by setting a `(?x)` option. This option enables including comments inside complicated patterns. Note, however, that this applies only to data characters. Whitespaces may not appear in special character sequences in a pattern, for example within the `(? (` sequence which introduces a conditional subpattern.

- ◆ Option 'm' is equivalent to `PCRE_MULTILINE`



By default, PCRE treats the subject string as consisting of a single line of characters (even if it actually contains newlines). The "start of line" metacharacter "^" matches only in the beginning of a string, while the "end of line" metacharacter "\$" matches only in the end of a string or before a terminating newline (unless `PCRE_DOLLAR_ENDONLY` is set).

When `PCRE_MULTILINE` is set, the "start of line" and "end of line" metacharacters match any newline characters which immediately follow or precede them in the subject string as well as in the very beginning and end of a subject string. This option can be changed within a pattern by a `(?m)` option setting. If there are no "\n" characters in the subject string, or ^ or \$ are not present in the pattern, the `PCRE_MULTILINE` option has no effect.

- ◆ Option 'u' is equivalent to `PCRE_UNGREEDY`

This option inverts the "greediness" of the quantifiers so that they are not greedy by default, but become greedy if followed by "?". The same result can also be achieved by the `(?U)` option in the pattern.

- ◆ Option 'd' is equivalent to `PCRE_DOTALL`

If this option is set, a dot metacharacter in the pattern matches all characters, including newlines. Without it, newlines are excluded. This option can be changed within a pattern by a `(?s)` option setting. A negative class such as `[^a]` always matches newline characters, regardless of the settings of this option.

- ◆ Option 'e' is equivalent to `PCRE_DOLLAR_ENDONLY`

If this option is set, a dollar metacharacter in the pattern matches only at the end of the subject string. Without this option, a dollar also matches immediately before a newline at the end of the string (but not before any other newline characters). The `PCRE_DOLLAR_ENDONLY` option is ignored if `PCRE_MULTILINE` is set.

J2. Peculiarities of PCRE Regular Expressions

A *regular expression* is a pattern that is matched against a subject string from left to right. Most characters stand for themselves in a pattern, and match the corresponding characters in the subject.

The power of regular expressions comes from the ability to include alternatives and repetitions in the pattern. These are encoded in the pattern by the use of metacharacters, which do not stand for themselves but instead are interpreted in a special way.

There are two different sets of metacharacters: those recognized anywhere in a pattern except within square brackets, and those recognized in square brackets. Outside square brackets, the metacharacters are as follows:

- \ general *escape* character with several uses,
- ^ assert start of string (or line, in multiline mode),
- \$ assert end of string (or line, in multiline mode),
- match any character except newline (by default),
- [start character class definition,
-] end character class definition,
- | start alternative branch,
- (start subpattern,
-) end subpattern,



- ? extends the meaning of (, also 0 or 1 quantifier, also quantifier minimizer.
- * 0 or more quantifier,
- + 1 or more quantifier, also "possessive quantifier",
- { start min/max quantifier.

Part of a pattern that is in square brackets is called a "character class". In a character class the only metacharacters are:

- \ general escape character,
- ^ negate the class, but only if the first character,
- indicates character range,
- [POSIX character class (only if followed by POSIX syntax),
-] terminates the character class.



Appendix K. Log Files Format

Events on the **Server** (see **Administrator Manual**, p. [Dr.Web Server Logging](#)) and the **Agent** are logged into a text file, where every line is a separate message.

The format of a message line is as follows:

```
<year><month><day> . <hour><minute><second> . <centisecond> <message_type> [<process_id>]  
<thread_name> [<message_source>] <message>
```

where:

- ◆ *<year><month><date>* . *<hour><minute><second>* . *<hundredth_of_second>* – exact date of message entry to the log file.
- ◆ *<message_type>* – log level:
 - **ftl (Fatal error)** – instructs to inform only of the most severe errors;
 - **err (Error)** – notify of operation errors;
 - **wrn (Warning)** – warn about errors;
 - **ntc (Notice)** – display important information messages;
 - **inf (Info)** – display information messages;
 - **tr0..3 (Trace, Trace 1, Trace 2, Trace 3)** – enable tracing events. The options are displayed in the ascending order according to the level of detail. Trace instructs to log in the minimum level of detail; **Trace 3** instructs to log in the maximum level of detail;
 - **db0..3 (Debug, Debug 1, Debug 2, Debug 3)** – instruct to log debugging events. The options are displayed in the ascending order according to the level of detail. Debug instructs to log in the minimum level of detail; **Debug 3** instructs to log in the maximum level of detail.



The **tr0..3 (trace)** and **db0..3 (debug)** levels of detail are applicable for messages for **Dr. Web Enterprise Security Suite** developers only.

- ◆ [*<process_id>*] – unique numerical identifier of the process within which the thread that wrote the message to the log file was executed. Under certain OS [*<process_id>*] may be represented as [*<process_id> <thread_id>*].
- ◆ *<thread_name>* – character representation of the thread within which the message was logged.
- ◆ [*<message_source>*] – name of the system that initiated logging the message. The source is not always present.
- ◆ *<message>* – text description according to the log level. It may include both a formal description of the event and the values of certain event-relevant variables.

For example,

```
1) 20081023.171700.74 inf [001316] mth:12 [Sch] Task "Purge unsent IS events"  
said OK
```

where:

- ◆ 20081023 – *<year><month><date>*,
- ◆ 171700 – *<hour><minute><second>*,
- ◆ 74 – *<hundredth_of_second>*,
- ◆ inf – *<message_type>*,
- ◆ [001316] – [*<process_id>*],
- ◆ mth:12 – *<thread_name>*,
- ◆ [Sch] – [*<message_source>*],



- ◆ Task "Purge unsent IS events" said OK – *<message>* about the correct performance of the **Purge unsent IS** events task.

2) 20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193

where:

- ◆ 20081028 – *<year><month><date>*,
- ◆ 135755 – *<hour><minute><second>*,
- ◆ 61 – *<hundredth_of_second>*,
- ◆ inf – *<message_type>*,
- ◆ [001556] – [*<process_id>*],
- ◆ srv:0 – *<thread_name>*,
- ◆ tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193 – *<message>* about having established a new connection through the specified socket.



Appendix L. Integration of Web API and Dr.Web Enterprise Security Suite



The **Web API** is described in the **Web API for Dr.Web® Enterprise Security Suite** manual.

Application

Web API, when integrated to **Dr.Web Enterprise Security Suite**, provides functions for operation of transactions with accounts and automatization of service users management. You can use it, for example, to create dynamic pages to receive requests from users and send them installation files.

Authentication

The HTTP(S) protocol is used to interact with **Dr.Web Server**. XML API accepts RESET requests and replies with the XML. To get access to the Web API, the Basic HTTP authentication is used (in compliance with [RFC 2617](#) standard). Contrary to RFC 2617 and related standards, the HTTP(S) server does not request credentials (i.e., **Dr.Web Enterprise Security Suite** administrator account name and its password) from the client.



Appendix M. Licenses

This section contains the list of third-party software libraries which are used by **Dr.Web Enterprise Security Suite** software, information on their licensing and development projects addresses.

Third-party library	License	Project URL
boost	http://www.boost.org/users/license.html *	http://www.boost.org/
bsdifff	Custom	http://www.daemonology.net/bsdifff/
c-ares	MIT License*	http://c-ares.haxx.se/
cairo	Mozilla Public License* GNU Lesser General Public License*	http://cairographics.org/
CodeMirror	MIT License*	http://codemirror.net/
fontconfig	Custom	http://www.freedesktop.org/wiki/Software/fontconfig
freetype	GNU General Public License* The FreeType Project License (BSD like)	http://www.freetype.org/
Gecko SDK	Mozilla Public License* GNU Lesser General Public License* GNU General Public License*	https://developer.mozilla.org/ru/docs/Gecko_SDK
GCC runtime libraries	GPLv3 or later with exception*	http://gcc.gnu.org/
htmlayout	Custom http://www.terrainformatica.com/htmlayout/prices.whtm	http://www.terrainformatica.com/htmlayout/
jQuery	MIT License* GNU General Public License*	http://jquery.com/
Leaflet	Custom	http://leafletjs.com
libcurl	http://curl.haxx.se/docs/copyright.html *	http://curl.haxx.se/libcurl/
libradius	© Juniper Networks, Inc.*	http://www.freebsd.org
libxml2	MIT License*	http://www.xmlsoft.org/
lua	MIT License*	http://www.lua.org/
lua-xmlreader	MIT License*	http://asbradbury.org/projects/lua-xmlreader/
lua4json	MIT License*	http://json.luaforge.net/
lzma	GNU Lesser General Public License* Common Public License (http://opensource.org/licenses/cpl1.0.php)*	http://www.7-zip.org/sdk.html
ncurses	MIT License*	https://www.gnu.org/software/ncurses/ncurses.html
Net-snmp	http://www.net-snmp.org/about/license.html *	http://www.net-snmp.org/
OpenLDAP	http://www.openldap.org/software/release/license.html *	http://www.openldap.org
OpenSSL	http://www.openssl.org/source/license.html *	http://www.openssl.org/
Oracle Instant Client	http://www.oracle.com/technetwork/licenses/instant-client-lic-152016.html *	http://www.oracle.com



Third-party library	License	Project URL
pcrc	http://www.pcre.org/license.txt *	http://www.pcre.org/
pixmap	MIT License*	http://pixmap.org/
Prototype JavaScript framework	MIT License*	http://prototypejs.org/assets/2009/8/31/prototype.js
script.aculo.us scriptaculous.js	Custom http://madrobby.github.io/scriptaculous/license/	http://script.aculo.us/
slt	MIT License*	http://code.google.com/p/slt/
SQLite	Public Domain (http://www.sqlite.org/copyright.html)	http://www.sqlite.org/
SWFUpload	MIT License*	http://code.google.com/p/swfupload/
wtl	Common Public License (http://opensource.org/licenses/cpl1.0.php)*	http://sourceforge.net/projects/wtl/
XML/SWF Charts	Bulk License (http://maani.us/xml_charts/index.php?menu=Buy)	http://www.maani.us/xml_charts/index.php?menu=Introduction
zlib	http://www.zlib.net/zlib_license.html *	http://www.zlib.net/

* - license texts are listed below.

M1. Boost

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

M2. Curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.



Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

M3. Libradius

Copyright 1998 Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

\$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro Exp \$

M4. Net-snmp

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved



Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.



* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc



All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----



Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) ----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

M5. OpenLDAP

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following
disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

M6. OpenSSL

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

=====

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:



```
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
=====
```

```
This product includes cryptographic software written by Eric Young  
(eay@cryptsoft.com). This product includes software written by Tim  
Hudson (tjh@cryptsoft.com).
```

```
Original SSLeay License
```

```
-----
```

```
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)  
All rights reserved.
```

```
This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).  
The implementation was written so as to conform with Netscapes SSL.
```

```
This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
```

```
Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
```

```
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
```

```
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.
```

```
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
```

```
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
```

```
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
```

```
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
```

```
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
```

```
The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
```

```
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
```

```
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
```



THIS SOFTWARE IS PROVIDED BY ERIC YOUNG 'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license

[including the GNU Public License.]

M7. Oracle Instant Client

Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement that you comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which the United States has prohibited export.

-You will not download or otherwise export or re-export the Programs, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries.

-You are not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are you listed on the United States Department of Commerce Table of Denial Orders.

You will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (<http://www.oracle.com/products/export>).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.



The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.



You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

- use the Programs for any purpose other than as provided above;
- charge your end users for use of the Programs;
- remove or modify any Program markings or any notice of our proprietary rights;
- assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;
- cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;
- disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at <http://www.oracle.com/products/export/index.html>. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.



IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. \$1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.



Last updated: 01/24/08

Should you have any questions concerning this License Agreement, or if you desire to contact Oracle for any reason, please write:

Oracle America, Inc.
500 Oracle Parkway,
Redwood City, CA 94065

Oracle may contact you to ask if you had a satisfactory experience installing and using this OTN software download.

M8. PCRE

PCRE is a library of functions to support regular expressions those syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk

University of Cambridge Computing Service,
Cambridge, England.

Copyright (c) 1997-2013 University of Cambridge
All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu

Copyright(c) 2010-2013 Zoltan Herczeg
All rights reserved.



STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg

Email local part: hzmester

Email domain: freemail.hu

Copyright(c) 2009-2013 Zoltan Herczeg

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007-2012, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

M9. Wtl

Common Public License Version 1.0



THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form.

This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.



c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION



Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.



All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

M10. Zlib

```
zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.8, April 28th, 2013
```

```
Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler
```

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

```
Jean-loup Gailly
```

```
Mark Adler
```

```
jloup@gzip.org
```

```
madler@alumni.caltech.edu
```

M11. MIT License

```
Copyright (c) <year> <copyright holders>
```



Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

M12. GNU General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.



For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.



The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.



When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.



c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, those source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.



When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.



Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.



If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.



If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

M13. GNU Lesser General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.



An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.



c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

M14. Mozilla Public License

Version 2.0

1. Definitions



1.1. "Contributor"

means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. "Contributor Version"

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor's Contribution.

1.3. "Contribution"

means Covered Software of a particular Contributor.

1.4. "Covered Software"

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. "Incompatible With Secondary Licenses"

means

that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. "Executable Form"

means any form of the work other than Source Code Form.

1.7. "Larger Work"

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. "License"

means this document.

1.9. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. "Modifications"

means any of the following:

any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

any new file in Source Code Form that contains any Covered Software.

1.11. "Patent Claims" of a Contributor



means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. "Secondary License"

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. "Source Code Form"

means the form of the work preferred for making modifications.

1.14. "You" (or "Your")

means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

for any code that a Contributor has removed from Covered Software; or

for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

under Patent Claims infringed by Covered Software in the absence of its Contributions.



This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices



You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability



Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at <http://mozilla.org/MPL/2.0/>.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - "Incompatible With Secondary Licenses" Notice



This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.

M15. GCC runtime libraries

COPYRIGHT STATEMENTS AND LICENSING TERMS

GCC is Copyright (C) 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 Free Software Foundation, Inc.

GCC is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3, or (at your option) any later version.

GCC is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

Files that have exception clauses are licensed under the terms of the GNU General Public License; either version 3, or (at your option) any later version.

The following runtime libraries are licensed under the terms of the GNU General Public License (v3 or later) with version 3.1 of the GCC Runtime Library Exception (included in this file):

- libgcc (libgcc/, gcc/libgcc2.[ch], gcc/unwind*, gcc/gthr*, gcc/coretypes.h, gcc/crtstuff.c, gcc/defaults.h, gcc/dwarf2.h, gcc/emults.c, gcc/gbl-ctors.h, gcc/gcov-io.h, gcc/libgcov.c, gcc/tsystem.h, gcc/typeclass.h).
- libdecnumber
- libgomp
- libssp
- libstdc++-v3
- libobjc
- libmudflap
- libgfortran
- The libgnat-4.4 Ada support library and libgnatvsn library.
- Various config files in gcc/config/ used in runtime libraries.

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Copyright (C) 2009 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.



This GCC Runtime Library Exception ("Exception") is an additional permission under section 7 of the GNU General Public License, version 3 ("GPLv3"). It applies to a given file (the "Runtime Library") that bears a notice placed by the copyright holder of the file stating that the file is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header files and runtime libraries with the compiled program. The purpose of this Exception is to allow compilation of non-GPL (including proprietary) programs to use, in this way, the header files and runtime libraries covered by this Exception.

0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for execution after a Compilation Process, or makes use of an interface provided by the Runtime Library, but is not otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications, governed by version 3 (or a specified later version) of the GNU General Public License (GPL) with the option of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and use would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor architecture, in executable form or suitable for input to an assembler, loader, linker and/or execution phase. Notwithstanding that, Target Code does not include data in any format that is used as a compiler intermediate representation, or used for producing a compiler intermediate representation.

The "Compilation Process" transforms code entirely represented in non-intermediate languages designed for human-written code, and/or in Java Virtual Machine byte code, into Target Code. Thus, for example, use of source code generators and preprocessors need not be considered part of the Compilation Process, since the Compilation Process can be understood as starting with the output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-compatible software, or if it is done without using any work based on GCC. For example, using non-GPL-compatible Software to optimize any GCC intermediate representations would not qualify as an Eligible Compilation Process.

1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime Library with Independent Modules, even if such propagation would otherwise violate the terms of GPLv3, provided that all Target Code was generated by Eligible Compilation Processes. You may then convey such a combination under terms of your choice, consistent with the licensing of the Independent Modules.

2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-party software is unaffected by the copyleft requirements of the license of GCC.



Chapter 3: Frequently Asked Questions

Moving Dr.Web Server to Another Computer (under Windows® OS)



After moving the **Server** to another computer, pay attention on transport protocols settings and, if necessary, edit corresponding settings in the **Administration** → **Dr.Web Server configuration** section, the **Transport** tab.

To transfer Dr.Web Server (for the similar Dr.Web Server versions) under Windows OS:

1. Stop the **Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
2. Run `drwcsd.exe` using the `exportdb` switch to export the content of the database to a file. The full command line (for Windows) looks as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" exportdb <file_path>
```

3. Backup the `C:\Program Files\DrWeb Server\etc` folder and the `drwcsd.pub` key from the `\Program Files\DrWeb Server\Installer` folder.
4. Remove **Dr.Web Server** software.
5. Install the new **Server** (empty, with the new DB) at the necessary computer. Stop the **Server** via the Windows OS service administrative loots or via **Dr.Web Security Control Center**.
6. Copy the automatic saved `etc` folder to the `C:\Program Files\DrWeb Server\etc` folder and the `drwcsd.pub` key to the `C:\Program Files\DrWeb Server\Installer` folder.
7. Run `drwcsd.exe` using the `importdb` switch to import the content of the database from a file. The full command line (for Windows) looks as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" importdb <file_path>
```

8. Start the **Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).



In case of using embedded DB, it is not necessary to export and import DB. Just save the `database.sqlite` file and replace the new DB file at the installed **Server** by an old DB file from the previous version of the **Server**.

To transfer Dr.Web Server (for the different Dr.Web Server versions) under Windows OS:

1. Stop the **Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
2. Save the database via the SQL server tools (in case of using embedded DB, just save the `database.sqlite` file).
3. Backup the `C:\Program Files\DrWeb Server\etc` folder and the `drwcsd.pub` key from the `\Program Files\DrWeb Server\Installer` folder.
4. Remove **Dr.Web Server** software.
5. Install the new **Server** (empty, with the new DB) at the necessary computer. Stop the **Server** via the Windows OS service administrative loots or via **Dr.Web Security Control Center**.
6. Copy the automatic saved `etc` folder to the `C:\Program Files\DrWeb Server\etc` folder and the `drwcsd.pub` key to the `C:\Program Files\DrWeb Server\Installer` folder.
7. Restore the DB on new **Server** and specify the path to the DB in the configuration file.



8. Run `drwcsd.exe` using the `upgradedb` switch to upgrade the database. The full command line (for Windows) looks as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" upgradedb "C:\Program Files\DrWeb Server\update-db"
```

9. Start the **Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).

If Dr.Web Server name or IP address is changed during the transfer:



For the possibility of transfer of **Agents** for which the new **Server** address is set via the **Control Center**, but not in the **Agent** settings at the station, keep both **Servers** operating till the procedure is completed.

1. Transfer the **Server** according to the corresponding procedure, described above.
2. For all **Agents**, which are served by transferred **Server**, specify the address of the new **Server** according to the procedure described in the [Connecting Dr.Web Agent to Other Dr.Web Server](#) section.

For the **Agents** for which the new **Server** address is set via the **Control Center**, but not in the **Agent** settings at the station, on both **Servers** in the **Agent** settings, the new **Server** IP address must be specified.

3. Wait until all **Agents** connect to the new **Server**. After this, you can remove the old **Server**.



Connecting Dr.Web Agent to Other Dr.Web Server

You can connect the **Agent** to the other **Server** by one of the following ways:

1. [Via the Control Center.](#)

Remote management without a direct access to the station is possible in case the station is still connected to the previous **Server**. You need the access to the **Control Center** both of the previous and the new **servers**.

2. [Directly at the station.](#)

To perform the actions directly on the station, you must have administrative permissions on the station and permissions to edit the **Agent** properties, which are set on the **Server**. If you do not have these permissions, you can reconnect to other **Server** locally on the station only after removing installed **Agent** and installing the new **Agent** with the new **Server** settings. If you do not have permissions to remove the **Agent** locally, use **Dr.Web Remover** utility to remove the **Agent** on the stations or remove the **Agent** via the **Control Center**.

To reconnect Dr.Web Agent to another Dr.Web Server via the Control Center

1. On the new **Server**, allow the stations with incorrect authorization parameters to request new authorization parameters as being newbies: select the **Administration** item of the main menu → the **Dr.Web Server configuration** item of the control menu → the **General** tab:
 - a) Set the **Reset unauthorized to newbie** flag if it is cleared.
 - b) If the option **Always deny access** is selected in the **Newbies registration** drop-down list, change it to the **Approve access manually** or **Allow access automatically**.
 - c) To apply these settings, click **Save** and reboot the **Server**.



If your company policy does not allow to change settings from the step 1, then you need to set the parameters of the station authorization, in accordance with the account created in advance in the **Control Center**, directly at the station.

2. On the old **Server** to which the **Agent** is connected, set the parameters of the new **Server**: select the **Anti-Virus Network** item of the main menu of the **Control Center** → select the required station (or the group for reconnecting all the stations of this group) in the hierarchical list of the network → the **Dr.Web Agent** option in the **Windows** section of the control menu → the **Network** tab:
 - a) If the `drwcsd.pub` public encryption key of the new **Server** does not match the encryption key of the previous **Server**, set the path to the new public key in the **Public key** field.
 - b) Set the new **Server** address in the **Server** field.
 - c) Click **Save**.

To reconnect Dr.Web Agent to another Dr.Web Server directly at the station

1. Set the new **Server** parameters in the **Agent** settings: in the context menu of the **Agent** icon, select: **Tools** → **Settings** → the **Main** tab → **Mode** → the **Connection to central protection server** section → the **Change** button:
 - a) If the `drwcsd.pub` public encryption key of the new **Server** does not match the encryption key of the old **Server**, set the path for the new public key in the **Public key** field.



If you cannot provide the new public key at the moment, you can set the **Use an invalid public key** flag to allow connection to the new **Server** with the old public key. In this case, after connection to the new **Server**, you need to provide a new public key via the **Control Center**, as described above, and clear the **Use an invalid public key** flag in the **Agent** settings.



- b) In the **Address** and the **Port** fields, set the corresponding parameters of the new **Server**.
2. Make the station a newbie (reset the authorization parameters on the **Server**): in the **Agent** settings section from the step 1, select: the **Advanced** section → click the **Connect as a newbie** button. Click **OK**.



If you already know the ID and the password to connect the new **Server**, you can provide them in the **Station ID** and the **Password** fields. In this case, there is no need to make the station a newbie.



Changing the Type of the DBMS for Dr.Web Enterprise Security Suite

For Windows OS

1. Stop **Dr.Web Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
2. Run `drwcsd.exe` using the `exportdb` switch to export the content of the database to a file. The full command line (for Windows) looks as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb D:\esbase.es
```

It is presumed that **Dr.Web Server** is installed to the `C:\Program Files\DrWeb Server` folder and the database is exported to a file `esbase.es`, which is in the root of disc `D`. Copy the line above to the clipboard and paste to the `cmd` file and run the file.

If the path to a file (or a file name) contains spaces or national characters, the path should be put in quotation marks:

```
"D:\<long name>\esbase.es"
```

3. Start **Dr.Web Server** (see the **Administrator Manual** p. [Start and Stop Dr.Web Server](#)), connect **Dr.Web Security Control Center** to the **Server** and configure the **Server** to use a different DBMS. Cancel restarting the **Server**.
4. Stop **Dr.Web Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
5. Run `drwcsd.exe` using the `initdb` switch to initialize a new database. The command line will look as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all initdb D:\Keys\agent.key -- root
```

It is presumed that the **Server** is installed to the `C:\Program Files\DrWeb Server` folder and `agent.key` resides in `D:\Keys`. Copy this line to the clipboard and paste to the `cmd` file. Run the file then.

If the path to a file (or a file name) contains spaces or national characters, the path to the key should be put in quotation marks:

```
"D:\<long name>\agent.key"
```

6. Run `drwcsd.exe` using the `importdb` switch to import the database from the file. The command line will look as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all importdb D:\esbase.es
```

Copy this line to the clipboard and paste to the `cmd` file. Run the file.

7. Start **Dr.Web Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).

For UNIX OS

1. Stop **Dr.Web Server** using the script



- ◆ for **Linux OS** and **Solaris OS**:

```
/etc/init.d/drwcsd stop
```

- ◆ for **FreeBSD OS**:

```
/usr/local/etc/rc.d/drwcsd.sh stop
```

or via **Dr.Web Security Control Center** (except the Solaris OS).

2. Start the **Server** with the `exportdb` switch to export the database to a file. The command line from the **Server** installation folder will look as follows:

- ◆ for **Linux OS**:

```
"/etc/init.d/drwcsd exportdb /var/esbase.es"
```

- ◆ For **Solaris OS**:

```
"/etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es"
```

- ◆ for **FreeBSD OS**:

```
"/usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/esbase.es"
```

It is presumed that the database is exported to `esbase.es`, which resides in the specified folder.

3. Start **Dr.Web Server** using the script

- ◆ for **Linux OS** and **Solaris OS**:

```
/etc/init.d/drwcsd start
```

- ◆ for **FreeBSD OS**:

```
/usr/local/etc/rc.d/drwcsd.sh start
```

connect **Dr.Web Security Control Center** to the **Server** and configure the **Server** to use another database through **Dr.Web Security Control Center** menu: **Administration** → **Dr.Web Server configuration** → **Database** tab.



You can also reconfigure the **Server** to use another database/DBMS by editing the **Server** configuration file `drwcsd.conf` directly. To do this, you should comment/delete the entry about the current database and enter the new database (for more details see [Appendix G1. Dr.Web Server Configuration File](#)).

You will be prompted to restart the **Server**. Reject restarting.

4. Stop **Dr.Web Server** (see step 1).
5. Run `drwcsd` using the `initdb` switch to initialize a new database. The command line will look as follows:

- ◆ for **Linux OS** and **Solaris OS**:

```
"/etc/init.d/drwcsd initdb /root/keys/agent.key - - root"
```

- ◆ for **FreeBSD OS**:

```
"/usr/local/etc/rc.d/drwcsd.sh initdb /root/keys/agent.key - - root"
```

It is presumed that the `agent.key` resides in the `/root/keys` folder.

6. Run `drwcsd` using the `importdb` switch to import the database from a file. The command line will look as follows:

- ◆ for **Linux OS** and **Solaris OS**:

```
"/etc/init.d/drwcsd importdb /var/esbase.es"
```

- ◆ for **Solaris OS**:



```
"/etc/init.d/drwcsd importdb /var/drwcs/etc/esbase.es"
```

◆ for **FreeBSD** OS:

```
"/usr/local/etc/rc.d/drwcsd.sh importdb /var/esbase.es"
```

7. Start **Dr.Web Server** (see step 3).



If you want to change the parameters at **Server** start (for example, specify the **Server** installation folder, change the log level, etc.), you will have to edit the start script:

- ◆ for **FreeBSD** OS: /usr/local/etc/rc.d/drwcsd.sh
- ◆ for **Linux** OS and **Solaris** OS: /etc/init.d/drwcsd



Restoring the Database of Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite regularly backs up important data (database contents, **Server** license key, private encryption key, **Server** configuration key, and **Dr.Web Security Control Center** configuration key). The backup files are stored in the following folders (relatively to the **Server** installation folder):

- ◆ for **Windows** OS: `\var\Backup`
- ◆ for **Linux** OS and **Solaris** OS: `/var/opt/drwcs/backup`
- ◆ for **FreeBSD**: `/var/drwcs/backup`

For that purpose a daily task is included to the **Server** schedule. If such task is missing, it is strongly recommended to create it.

The copies are stored in the `.gz` format unpackable with `gzip` and other archivers. After unpacking all the files, except for the database contents, are ready to use. To restore the data, the database contents can be imported from the backup to another database of the **Server** by means of the `importdb` switch.

Restoring the DB for Different Versions of Dr.Web Server

You can restore the DB from the backup copy only if it had been created via the **Server** of the same major version as the version of the **Server** which you use for restoring.

For example:

- ◆ You can restore DB from the backup created via the **Server** of **5.0** version using the **Server** of **5.0** version only.
- ◆ You can restore DB from the backup created via the **Server** of **6.0** version using the **Server** of **6.0** version only.
- ◆ You cannot restore DB from the backup created via the **Server** of **5.0** or **4.XX** version using the **Server** of **6.0** version.

If DB has been corrupted for some reasons during Server upgrade from previous versions to 6.0 version, do the following:

1. Remove the **Server** software of **6.0** version. Backup copies of files, used by the **Server**, will be stored automatically.
2. Install the **Server** of version, which had been installed before upgrading and had been used to create backup copy.

According to the general upgrade procedure, you should use all stored **Server** files except the DB file.

Create a new DB during the **Server** installation.

3. Restore DB from the backup according to general rules (see procedures [below](#)).
4. Disable the **Agent**, the **Server** and the **Network Installer** protocols in the **Server** settings. To do this, select the **Administration** item in the main menu and click **Dr.Web Server configuration** in the control menu, go to the **Modules** tab and clear corresponding flags.
5. Upgrade the **Server** to the **6.0** version according to general rules (see **Administrator Manual**, p. [Updating Dr.Web Enterprise Security Suite Software and Its Components](#)).
6. Enable the **Agent**, the **Server** and the **Network Installer** protocols, disabled at the step 4.



For Windows OS

To restore DB from backup:

1. Stop **Dr.Web Server** (if it is running, see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
2. Import the content of the database from the correspondent backup file. The command line will look as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all importdb "<path_to_the_backup_file>\database.gz"
```

The command must be entered in a single line. It is presumed that **Dr.Web Server** is installed to the C:\Program Files\DrWeb Server folder.

3. Start **Dr.Web Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).

To restore DB from backup in case of changing Dr.Web Server version or corruption of the previous DB version:

1. Stop **Dr.Web Server** (if it is running, see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).
2. Remove the current DB. To do this:
 - 2.1. For the embedded DB:

a) Remove `database.sqlite` file.

b) Initialize a new database. In Windows the command line will look as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all initdb D:\Keys\agent.key - - <password>
```

The command must be entered in a single line. (See also `drwcsd` command format with the `initdb` switch at the [Appendix H3.3.](#)). It is presumed that **Dr.Web Server** is installed to the C:\Program Files\DrWeb Server folder and `agent.key` is located in D:\Keys.

c) Once this command is executed, a new `database.sqlite` of about 200 Kb will be generated in the `var` subfolder of **Dr.Web Server** installation folder.

2.2. For the external DB: cleanup the DB via the `clean.sql` script, located in the `etc` subfolder of **Dr.Web Server** installation folder.

3. Import the content of the database from the correspondent backup file. The command line will look as follows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all importdb "<disc:>\<path_to_the_backup_file>\database.gz"
```

The command must be entered in a single line. It is presumed that **Server** is installed to the C:\Program Files\DrWeb Server folder.

4. Start **Dr.Web Server** (see **Administrator Manual**, p. [Start and Stop Dr.Web Server](#)).

For UNIX OS

1. Stop **Dr.Web Server**.
 - ◆ for **Linux OS** and **Solaris OS**:



```
/etc/init.d/drwcsd stop
```

- ◆ for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh stop
```

- ◆ for **other** supported versions:

```
/bin/drwcs.sh stop
```

2. Remove `database.sqlite` from the

- ◆ for **Linux** OS and **Solaris** OS:

```
/var/opt/drwcs/
```

- ◆ for **FreeBSD** OS:

```
/var/drwcs/
```

subfolder of the **Server** installation folder.



To clean an external DB, use the `clean.sql` script, located at:

- ◆ `/var/opt/drwcs/etc` for **Linux** OS and **Solaris** OS,
- ◆ `/var/drwcs/etc` for **FreeBSD** OS.

3. Initialize the **Server** database. The command will look as follows:

- ◆ for **Linux** OS and **Solaris** OS:

```
/etc/init.d/drwcsd initdb
```

- ◆ for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh initdb
```

- ◆ for **other** supported versions:

```
su drwcs -c "bin/drwcsd -var-root=./var -verbosity=all -log=./var/server.log  
initdb etc/agent.key - - <password>"
```

4. Once this command is executed, a new `database.sqlite` database of about 200 Kb will be generated in the `var` subfolder of **Dr.Web Server** installation folder.

5. Import the content of the database from the correspondent backup. The command line will look as follows:

- ◆ for **Linux** OS and **Solaris** OS:

```
/etc/init.d/drwcsd importdb "<path_to_the_backup_file>/database.gz"
```

- ◆ for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh importdb "<path_to_the_backup_file>/database.gz"
```

- ◆ for **other** supported versions:

```
bin/drwcsd -var-root=./var -verbosity=all -log=logfile.log importdb "<path_to_the_backup_file>/database.gz"
```

6. Start **Dr.Web Server**:

- ◆ for **Linux** OS and **Solaris** OS:

```
/etc/init.d/drwcsd start
```

- ◆ for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh start
```

- ◆ for **other** supported versions:

```
/bin/drwcs.sh start
```



If you want to run the script with parameters (e.g., set **Server** installation directory, change log details level and etc.), you must make all changes in the start script:

- ◆ for **FreeBSD** OS: `/usr/local/etc/rc.d/drwcsd.sh`
 - ◆ for **Linux** and **Solaris** OS: `/etc/init.d/drwcsd`
-

If some **Agents** were installed after the last backup had been made they will not be connected to the **Server** after the database has been restored from the backup. You should remotely reset them to the newbie mode. To do this, on **Dr.Web Security Control Center Administration** menu, select **Configure Server**. **Dr.Web Server configuration** window will be opened on the **General** tab. Set the **Reset unauthorized to newbie** flag.

As soon as the database is restored from the backup it is recommended to connect **Dr.Web Security Control Center** to the **Server**. On the **Administration** menu, select **Dr.Web Server Task Scheduler** and check that the **Back up critical server data** task is on the list. If this task is absent, add it to the list.



Restoring Dr.Web Server from Data Backup

Dr.Web Enterprise Security Suite regularly backs up important data: database contents, **Server** license key, private encryption key, **Server** configuration key, and **Dr.Web Security Control Center** configuration key. The backup files are stored in the following folders (relatively to the **Server** installation folder):

- ◆ for **Windows** OS: `\var\Backup`
- ◆ for **Linux** OS and **Solaris** OS: `/var/opt/drwcs/backup`
- ◆ for **FreeBSD**: `/var/drwcs/backup`

For that purpose a daily task is included to the **Server** schedule. If such task is missing, it is strongly recommended to create it.

The copies are stored in the `.gz` format unpackable with `gzip` and other archivers. After unpacking all the files, except for the database contents, are ready to use. To restore the data, the database contents can be imported from the backup to another database of the **Server** by means of the `importdb` switch (see p. [Restoring the Database of Dr.Web Enterprise Security Suite](#)).

It is also recommended to store copies of the following files on another PC: `drwcsd.pri` and `drwcsd.pub` encryption keys, license keys, `certificate.pem` SSL certificate, `private-key.pem` RSA private key and regularly copy **Server** database contents backup `database.gz`, **Server** and **Dr.Web Security Control Center** configuration files `drwcsd.conf` and `webmin.conf` to another PC. Thus you will be able to avoid data loss should the PC, on which **Dr.Web Server** is installed, be damaged, and to fully restore the data and the functionality of the **Server**. If license keys are lost they may be requested once again, as specified in **Administrator Manual**, p. [Key Files](#).

To Restore Dr.Web Server for Windows OS

Install **Dr.Web Server** software of the same version as the lost one on a working PC (see **Installation Manual**, p. [Installing Dr.Web Server for Windows® OS](#)). During the installation:

- ◆ If there is a copy of the DB (embedded or external) on another PC and it is not damaged, in the respective dialog boxes of the installer specify it along with the saved files of the **Server** license key, private encryption key and **Server** configuration.
- ◆ If the **Server** DB (embedded or external) was lost, but a backup of its contents `database.gz` is saved, then in the respective dialog boxes of the installer select creating a new database, specify the saved files of the **Server** and **Agent** license keys, private encryption key and **Server** configuration. After the installation import the DB contents from the backup (see p. [Restoring the Database of Dr.Web Enterprise Security Suite](#)).

To Restore Dr.Web Server for UNIX System-Based OS

1. Install **Dr.Web Server** software of the same version as the lost one on a working PC (see **Installation Manual**, p. [Installing Dr.Web Server for UNIX® System-Based OS](#)).
2. Put the saved files to:
 - ◆ for **Linux** OS: `/var/opt/drwcs/etc`, except for the public key. Put the latter to `/opt/drwcs/Installer/`
 - ◆ for **FreeBSD** OS: `/var/drwcs/etc`, except for the public key. Put the latter to `/usr/local/drwcs/Installer/`
 - ◆ for **Solaris** OS: `/var/drwcs/etc`, except for the public key. Put the latter to `/opt/drwcs/Installer/`



For all replaced files assign the same permissions as those set at the previous (lost) installation of the **Server**.

3. Generate a new SSL certificate:

- ◆ for **Linux OS** and **Solaris OS**:

```
/etc/init.d/drwcsd selfcert
```

- ◆ for **FreeBSD OS**:

```
/usr/local/etc/rc.d/drwcsd.sh selfcert
```

- ◆ for **other** supported versions:

```
/opt/drwcs/bin/drwcsd -var-root=/var/drwcs -log=/var/drwcs/log/drwcsd.log  
selfcert
```

4. The next steps depend on the availability of the **Server** database:

- If you have a working external DB, no further restoring procedures are needed, provided that you have the configuration file and the **Server** build is the same as the old one. Otherwise you will have to register the database in the configuration file and/or update the structure of the database with the `upgradedb` switch (see variant **c** below).
- If you have a backup of embedded or external DB contents (`database.gz`), start the **Server**, remove the embedded DB created at the installation, initiate creating a new one and import the contents of the old DB from the backup copy (see p. [Restoring the Database of Dr.Web Enterprise Security Suite](#)).
- If you have a saved copy of the embedded DB, replace the new file with it:
for **Linux OS** and **Solaris OS**: `/var/opt/drwcs/database.sqlite`
for **FreeBSD OS**: `/var/drwcs/database.sqlite`



For all replaced files assign the same permissions as those set at the previous (lost) installation of the **Server**.

To upgrade the databases, execute the following commands:

for **Linux OS** and **Solaris OS**:

```
/etc/init.d/drwcsd upgradedb
```

for **FreeBSD OS**:

```
/usr/local/etc/rc.d/drwcsd.sh upgradedb
```

for **other** supported versions:

```
/opt/drwcs/bin/drwcsd -var-root=/var/drwcs -log=/var/drwcs/log/drwcsd.log  
upgradedb update-db
```

5. Launch **Dr.Web Server**.



If some **Agents** were installed after the last backup had been made they will not be connected to the **Server** after the database has been restored from the backup. You should remotely reset them to the newbie mode. For that purpose, on **Dr.Web Security Control Center Administration** menu, select **Dr.Web Server configuration**. The **Dr.Web Server configuration** window will be opened. On the **General** tab, set the **Reset unauthorized to newbie** flag.



Upgrading Dr.Web Agents on the LAN servers

When upgrading **Agents** installed on the LAN servers, restarting stations or stopping a network software on such stations can be unwanted.

To avoid functionality downtime of stations that implement significant network functions, the following upgrading mode of **Agents** and anti-virus software is recommended:

1. In the **Server** schedule, change standard tasks for upgrading all components to upgrading virus bases only.
2. Create a new task for upgrading all components at the suitable time, when it will not be critical for LAN servers functionality.

How to create and edit tasks in the **Server** schedule, described in the **Administrator Manual**, p. [Setting Dr.Web Server Schedule](#) section.



It is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on servers those implement significant network functions (domain controllers, license distribution servers and etc.) to avoid probable conflicts between network services and internal components of **Dr.Web** anti-virus.



Restoring the Password of Dr.Web Enterprise Security Suite Administrator

If the administrative password for access to **Dr.Web Server** is lost, you can view or change it by direct access to the **Server** DB:

- a) For an embedded DB, to view and change administrative password, use the `drwidbsh` utility, which is included in the **Server** distribution kit.
- b) For an external DB, use corresponding `sql` client.



Parameters of administrative accounts are stored in the `admins` table.

Example of using the `drwidbsh` utility

1. Run the `drwidbsh3` utility and specify the path to the DB file:

- ◆ For the embedded DB under Linux OS:

```
/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
```

- ◆ For the embedded DB under Windows OS:

```
"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb Server\var\database.sqlite"
```



If you use embedded database of an old IntDB format, e.g., in case of the **Server** upgrade from the **6** version, when default database name is `dbinternal.dbs`, and database management utility is `drwidbsh`.

2. To view all data from the `admins` table, run the following command:

```
select * from admins;
```

3. To view logins and passwords of all administrative accounts, run the following command:

```
select login,password from admins;
```

4. If only one account with the `admin` name exists and it has the `root` password, you will get the following result:

```
sqlite> select login,password from admins;
admin|root
sqlite> █
```

5. To change the password, use the `update` command. In the following example, the command changes the password of the `admin` account to `qwerty`:

```
update admins set password='qwerty' where login='admin';
```

6. To exit the `drwidbsh` utility, run the following command:

```
.exit
```

Description of the `drwidbsh` utility is given in the appendix [H6. The Administrating Utility of the Embedded Database](#).



Using DFS During Installation of the Agent via the Active Directory

During installation of **Dr.Web Agent** via the Active Directory service, you can use Distributed File System (DFS).

It can be useful, for example, for several domain controllers in LAN.

For installation in the LAN with several domain controllers:

1. Create directory with the same name on each domain controller.
2. Via the DFS, unite created directories to one root destination directory.
3. Perform the administrative installation of the *.msi package to the created destination directory (see **Installation Manual**, p. [Installing Dr.Web Agent Software via Active Directory](#)).
4. Use this destination directory during package assignment in the group policy object editor.

Use the network address as: \\<domain>\<folder>

where: <domain> - the domain name, <folder> - the name of destination directory.



Chapter 4: Remote Installation Trouble Shooting

Principle of the installation:

1. The browser (**Dr.Web Security Control Center Extension** module) connects to the ADMIN\$ resource at the remote station (\\<remote_station>\ADMIN\$\Temp) and copies installer files (drwinst.exe, drwcsd.pub), specified in **Dr.Web Security Control Center** to the \\<remote_station>\ADMIN\$\Temp folder.
2. The extension runs drwinst.exe file at the remote station with the switches according to **Dr.Web Security Control Center** settings.

Successful installation requires that at the station from which the installation will be performed:

1. The ADMIN\$\Temp resource must be available at the remote station.

The availability can be checked in the following way:

In the address line of the Windows Explorer application, enter the following:

```
\\<remote_station>\ADMIN$\Temp
```

You will get the prompt for entering login and password for access to this resource. Enter the account data, which have been specified on the installation page.

The ADMIN\$\Temp resource can be unavailable for the following reasons:

- a) account does not have administrative rights;
 - b) the station is powered off or firewall blocks access to the 455 port;
 - c) limitations of remote access to the ADMIN\$\Temp resource at the Windows Vista and later OS, if the station is outside a domain;
 - d) the folder owner is absent or not enough privileges on the folder for the user or the group.
2. The drwinst.exe and drwcsd.pub files are available.

At **Dr.Web Security Control Center**, the external information (step and error code), which can help to diagnose the error reason, is displayed.

The list of the most frequently errors

Step	Error Code	Reason
Validating user inputs of the remote stations (1)	No such host is known (11001).	DNS name to address conversion failed. No such DNS name or wrong name server settings.
Checking if NetBIOS on the remote station is available (2)	A socket operation failed because the destination host was down (10064).	445 port is not available at the remote station. Possible reasons: <ul style="list-style-type: none"> ◆ station is shut down; ◆ firewall blocks specified port; ◆ the OS at the remote station is different from the Windows OS.
Connecting to an administrative resource ADMIN\$ on the remote station (1001)	At this step, connection with the ADMIN\$ administrative resource at the remote station is performed.	



Step	Error Code	Reason
	The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you (1265).	<ul style="list-style-type: none">◆ Sharing and security model for local accounts is not configured.◆ Authorization server is not available (domain controller).
	Logon failure: unknown user name or bad password (1326).	Unknown user name or bad password.
	The filename, directory name, or volume label syntax is incorrect (123).	The ADMIN\$ resource does not exist at the remote station.
Checking installer exit code (1009)	At this step, result of installation is checked.	
	Unknown error (2).	Ask for the technical support of the Doctor Web company.
	Installation is not required on this computer (4).	The Agent is already installed or has been incorrectly deleted (in this case, use the drwebremover utility) at this station.
	Protocol violation (6).	The drwinst.exe installer is not matched with the Server version. Make sure, that the installer is from the Server installation package.
	Cannot initialize scripting engine (7).	System error. Ask for the technical support of the Doctor Web company.
	Connection to server timed out (8).	Dr.Web Server is not available from the remote station.
	System should be rebooted to finish previous deinstallation (9).	Restart the station to complete previously uninstallation.



Index

A

- anti-virus Scanner 84
- anti-virus Server
 - configuration file 49
 - moving 137
 - restoring 148
 - start instruction switches 75

B

- backup
 - anti-virus Server 148
 - DB (database) 144
- billing system 98

C

- configuration file
 - anti-virus server 49
 - Control Center 62
 - proxy server 67
- Control Center
 - configuration file 62

D

- DB (database)
 - backup files 144
 - DBMS 141
 - internal 14
 - Oracle 17
 - PostgreSQL 19
 - restoring 144
- DMBS settings 14
- Dr.Web Server
 - configuration file 49
 - moving 137
 - restoring 148
 - start instruction switches 75

E

- encryption
 - key files, generating 83
- environment variables 92

K

- key files
 - encryption, generating 83

N

- Network
 - Installer 71
- network addresses 40
 - Dr.Web Agent/ Installer 42
 - Dr.Web Server 41
- notifications
 - templates parameters 34

P

- proxy server
 - configuration file 67

R

- regular expressions 93, 94
- restoring
 - anti-virus Server 148
 - DB (database) 144

S

- Scanner
 - anti-virus 84
- switches, start instruction
 - anti-virus Server 75
 - Network Installer 71
- system requirements 9

