Dr.WEB

Enterprise Security Suite

Appendices

Trademarks

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 13.0
Appendices
1/12/2022

Doctor Web Head Office

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

Website: https://www.drweb.com/

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

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions 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 anti-virus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

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

Table of Contents

Chapter 1: Introduction

About Manual

Documentation for Dr.Web Enterprise Security Suite anti-virus network administrator is intended to introduce general features and provide detailed information on delivering comprehensive anti-virus protection of a company's computers using Dr.Web Enterprise Security Suite.

Documentation for anti-virus network administrator contains the following parts:

1. **Installation Manual**

   Installation Manual will be useful to a company manager who makes the decision to purchase and install a system of comprehensive anti-virus protection.

   Installation Manual explains how to build an anti-virus network and install its main components.

2. **Administrator Manual**

   Administrator Manual is meant for *anti-virus network administrator*—the employee of a company who is responsible for anti-virus protection of computers (workstations and servers) of this network.

   An anti-virus network administrator should either have a system administrator privileges or work closely with a local network administrator, be competent in anti-virus protection strategy, and know every detail of Dr.Web anti-virus packages for all operating systems that are used in the network.

3. **Appendices**

   Appendices provide technical information describing configuration parameters for Anti-virus components and the syntax and values of instructions used to work with these modules.

   > ⚠ Above-mentioned documents have cross-references between them. When you download these documents to a local computer, cross-references will work as long as the documents are placed in the same folder, under their initial names.

In addition, the following Manuals are provided:

1. **Anti-virus Network Quick Installation Guide**

   Brief information on installation and initial configuration of anti-virus network components. For detailed information refer to administrator documentation.

2. **Manuals on managing the workstations**

   Details about centralized configuration of anti-virus software on workstations, which is to be provided by an anti-virus network administrator via the Dr.Web Security Control Center.

3. **User Manuals**

Details about Dr.Web anti-virus software configuration, when made on protected stations directly.

4. **Web API Manual**

   Technical details on integration of Dr.Web Enterprise Security Suite with third-party software via Web API.

5. **Dr.Web Server Database Manual**

   Description of internal structure of Dr.Web Server database and examples of its usage.

All the listed Manuals are also provided as a part of Dr.Web Enterprise Security Suite product and can be opened from the Dr.Web Security Control Center.

Before reading these documents, make sure you have the latest version of the corresponding Manuals for your product version. The Manuals are constantly updated and the latest version can be always found at the official website of Doctor Web at https://download.drweb.com/doc/.

Conventions and Abbreviations

Conventions

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

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

Abbreviations

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

- ACL—Access Control List,
- CDN—Content Delivery Network,
- DFS—Distributed File System,
- DNS—Domain Name System,
- FQDN—Fully Qualified Domain Name,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- MIB—Management Information Base,
- MTU—Maximum Transmission Unit,
- NAP—Network Access Protection,
- TTL—Time To Live,
- UDS—UNIX Domain Socket,

- DB, DBMS—Database, Database Management System,
- Dr.Web GUS—Dr.Web Global Update System,
- LAN—Local Area Network,
- OS—Operating System.

Chapter 2: Appendices

Appendix A. The Complete List of Supported OS Versions

For Dr.Web Server and Dr.Web Proxy Server

UNIX system-based OS

Linux using the `glibc` library 2.13 or later, including:

- ALT Linux 8
- ALT Linux 9
- Astra Linux Special Edition (Smolensk) 1.5 (with cumulative patch 20201201SE15)
- Astra Linux 1.6 (with cumulative patch 20200722SE16)
- Astra Linux 1.7
- Astra Linux Common Edition 2.12 Orel
- ALT 8 SP
- GosLinux IC6

⚠ In ALT 8 SP and GosLinux IC6 mandatory access control is not supported.

FreeBSD 11.3 or later.

Windows OS

- 32 bit:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

- 64 bit:

- Windows Server 2008 R2
- Windows 7
- Windows Server 2012
- Windows Server 2012 R2
- Windows 8

- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

For Dr.Web Scanning Server

You can install Dr.Web Scanning Server on a virtual machine that meets the following requirements:

Component	**Requirement**
Hypervisor	**VMware**, **Hyper-V**, **Xen, KVM**
Operating System	**Linux, FreeBSD.** The list of operating systems is the same as the list for anti-virus package for UNIX OS.
CPU	CPU with the following architecture and command system • Intel/AMD: 32-bit (IA-32, x86) and 64-bit (x86_64, x64, AMD64)
RAM	At least 500 Mb of free RAM (1 Gb or more is recommended).
Hard disk space	At least 1 GB of free disk space.
Network connections	Availability of network connections: • Valid Internet connection to enable updates for virus databases and filter database • Connection for processing requests from Virtual Agents to the service VM.

For Dr.Web Agent and Anti-Virus Package

UNIX system-based OS

Component	**Requirement**
Platform	Processors of the following architectures and command systems are supported: • **Intel/AMD**: 32-bit (*IA-32, x86*); 64-bit (*x86-64, x64, amd64*) • **ARM64**

Component	Requirement
	• **E2K** *(Elbrus)*
RAM	At least 500 Mb of free RAM (1 Gb or more is recommended).
Space on hard disk	At least 2 ГВ of free disk space on the volume where application directories are stored.
Operating system	• **FreeBSD** 11, 12. • **Linux** based on kernel ver. 2.6.37 or later, and using the **glibc** library ver. 2.13 or later. The supported **Linux** distributions are listed below. Operation system must support the **PAM** authentication mechanism. For the correct operation of SpIDer Gate, OS kernel must be built with inclusion of the following options: • *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;* • *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;* • *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.* The set of required options from the specified list can depend on the used distribution kit of **GNU/Linux**.
Other	The following valid network connections: • Valid Internet connection to enable updates for virus databases and application components. • When operating in the central protection mode, connection to the server on the local network is enough; connection to the Internet is not required.

For systems operating on 64-bit platforms, support of 32-bit applications must be enabled.

For **FreeBSD** OS, applicatio can be installed only from the universal package.

The product is supported for the following **Linux** distributions:

Platform	Supported Linux distributions
x86_64	- Astra Linux Special Edition (Smolensk)1.5 (with cumulative patch 20201201SE15), 1.6 (with cumulative patch 20200722SE16), 1.7 - Astra Linux Common Edition 2.12 Orel - Debian 9, 10 - Fedora 31, 32 - CentOS 7, 8 - Ubuntu 18.04, 20.04 - ALT Workstation 8, 9 - ALT Server 8, 9 - ALT 8 SP - RED OS Murom 7.2, 7.3 - GosLinux IC6 - SUSE Linux Enterprise Server 12SP3 - Red Hat Enterprise Linux 7, 8
x86	- CentOS 7 - Debian 10 - ALT 8 SP - ALT Workstation 9
ARM64	- Ubuntu 18.04 - CentOS 7, 8 - ALT 8 SP - ALT Workstation 9 - ALT Server 9
E2K	- Astra Linux Special Edition (Leningrad) 8.1 (with cumulative patch 8.120200429SE81) - ALT 8 SP - Elbrus-D MCST 1.4 - GS CS Elbrus 8.32 TVGI.00311-28

⚠ In ALT 8 SP, Astra Linux Special Edition (Novorossiysk) 4.11 and GosLinux IC6 mandatory access control is not supported.

For other Linux distributions that meet the above-mentioned requirements full compatibility with application is not guaranteed. If a compatibility issue occurs, If a compatibility issue occurs, contact technical support.

Windows OS

- 32 bit:

- Windows XP with SP2
- Windows Server 2003 with SP1
- Windows Vista with SP2
- Windows Server 2008 with SP2
- Windows 7 with SP1
- Windows 8
- Windows 8.1
- Windows 10, version 21H2 or earlier

- 64 bit:

- Windows Vista with SP2
- Windows 7 with SP1
- Windows 8
- Windows 8.1
- Windows 10, version 21H2 or earlier
- Windows 11
- Windows Server 2008 with SP2
- Windows Server 2008 R2 with SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

As Microsoft has stopped supporting the SHA-1 hashing algorithm, please ensure that your operating system supports the SHA-256 hashing algorithm before installing Dr.Web Agent on Windows Vista, Windows 7, Windows Server 2008 or Windows Server 2008 R2. To do this, install all the recommended updates listed in Windows Update. Please visit Doctor Web official website for details.

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

macOS

OS X 10.11 El Capitan

macOS 10.12 Sierra

macOS 10.13 High Sierra

macOS 10.14 Mojave

macOS 10.15 Catalina

macOS 11.5 BigSur

macOS 12 Monterey

Android OS

Android 4.4

Android 5.0

Android 5.1

Android 6.0

Android 7.0

Android 7.1

Android 8.0

Android 8.1

Android 9.0

Android 10.0

Android 11.0

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

> **Dr.Web Server database structure** is available in the form of a separate manual of the same name. The document can be opened from the **Support** section in Dr.Web Security Control Center.

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

Name	Default value	Description
DBFILE	database.sqlite	Path to the database file
CACHESIZE	2048	Database cache size in pages
PRECOMPILEDCACHE	1048576	Cache size of precompiled sql operators (in bytes)
MMAPSIZE	• 10485760—for UNIX, • 0—for Windows	Maximum size of the database file (in bytes) that is allowed to be mapped into process address space at a time.
CHECKINTEGRITY	QUICK	Verify integrity of the database image at Dr.Web Server startup: • FULL—full check for any errors concerning UNIQUE, CHECK, and NOT NULL constraints, malformed records, missing pages or index inconsistencies. • QUICK—fast check option, with no regards to constraint errors or index inconsistencies, • NO—integrity check is disabled.
AUTOREPAIR	NO	Automatically restore corrupted database image at Dr.Web Server startup: • YES—the database image restoration is initiated each time Dr.Web Server starts, • NO—automatic restoration is disabled.
WAL	YES	Use Write-Ahead Logging: • YES—true, • NO—false.
WAL-MAX-PAGES	1000	Max number of “dirty” pages. When reached, the pages will been written on disk.
WAL-MAX-SECONDS	30	Max time in seconds that the page writing on disk is delayed for.

SYNCHRONOUS	FULL	Mode of synchronous logging of changes in the database to the disk: • FULL—fully synchronous logging to the disk, • NORMAL—synchronous logging of critical data, • OFF—asynchronous logging.

The SQLite3 DBMS are provided as embedded—DBMS that is supported by Dr.Web Server starting from version 10.

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 B3. 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).

Microsoft SQL Server 2008 and later is supported. Microsoft SQL Server 2014 and later is recommended to use.

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 Dr.Web Server under UNIX system-based OS, the proper operation via the ODBC with FreeTDS is not guaranteed.

If warnings or errors occur in Dr.Web Server interaction with Microsoft SQL Server DBMS via the ODBC, please make sure that you are using the latest available DBMS version for this edition.

How to determine updates level, you can find on the following page of Microsoft corporation: https://docs.microsoft.com/en-US/troubleshoot/sql/general/determine-version-edition-update-level.

To reduce a number of deadlocks when using Microsoft SQL Server DBMS with the default transaction isolation level (READ COMMITTED), it is recommended that you enable the READ_COMMITTED_SNAPSHOT option by running the following SQL command:

```
ALTER DATABASE <database_name>
SET READ_COMMITTED_SNAPSHOT ON;
```

The command above shall be run in implicit transaction mode and with a single existing connection to the database.

Comparison Characteristics

⚠ An embedded DB can be used, if at most 200-300 stations are connected to Dr.Web 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 Dr.Web 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.
- When using embedded DB, you do not need to install components of third-party software. It is recommended mainly for the typical use of databases.
- Embedded database does not require DBMS administration skills and is a good choice for anti-virus network of small and medium sizes.
- 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 (specific values are given for example).

Table B-2. Parameters for ODBC connection

Name	Value	Description
DSN	drwcs	Data set name

Name	Value	Description
`USER`	`drwcs`	User name
`PASS`	`fUqRbrmlvI`	Password
`TRANSACTION`	`DEFAULT`	Possible values of the `TRANSACTION` parameter: • `SERIALIZABLE` • `READ_UNCOMMITTED` • `READ_COMMITTED` • `REPEATABLE_READ` • `DEFAULT` The `DEFAULT` value means "use default of the SQL server". More information on transactions isolation see in documentation on corresponding DBMS.

⚠ 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 data**—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.

When creating a new database in the Microsoft SQL DBMS, you must specify the collation that is case sensitive (has the `_CS` suffix) and accent-sensitive (has the `_AS` suffix).

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 sytem-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 Dr.Web 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 Dr.Web Server, in the installer settings, 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.

Connection to the Oracle database as the SYS and SYSTEM users, and also with the SYSDBA and SYSOPER privileges is forbidden.

Installation and Supported Versions

To use Oracle as en 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 website of the vendor.

Platforms supported by the Oracle Client are listed on the website of the vendor.

Dr.Web Enterprise Security Suite supports the Oracle DBMS of version 11 and later.

Also, please note the system requirements for Dr.Web Server when operating with the Oracle external database (see **Installation Manual**, p. System Requirements).

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 Dr.Web 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 use PostgreSQL as an external database

1. Install the PostgreSQL or Postgres Pro 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: in the **Dr.Web Server configuration** menu, the **Database** tab.

   ⚠ To connect to the PostgreSQL DB you can use only trust, password and MD5 authorization.

Installation and Supported Versions

1. Download the latest available version of this PostgreSQL free product (the PostgreSQL server and correspondent ODBC-driver), otherwise do not use the version earlier than **8.4** or 11.4.1 for Postgres Pro.
2. Create the PostgreSQL database by one of the following ways:

   a) Using the `pgAdmin` graphical interface.

   b) Using the `CREATE DATABASE` SQL command.

   ⚠ Database must be created in the UTF8 encoding.

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

Also, please note the system requirements for Dr.Web Server when operating with the PostgreSQL external database (see **Installation Manual**, p. System Requirements).

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 Dr.Web Server
`requiressl`		• 1 instructs to request a SSL connection • 0 does not instruct to make the request
`temp_tablespaces`		Name space for temporary tables
`default_transaction_isolation`		Transaction isolation mode (see PostgreSQL documentation)

More information can be found at https://www.postgresql.org/docs/.

Dr.Web Server and PosrtgreSQL 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.

Configuring the PostgreSQL Database

To increase performance during interaction with the PostgreSQL database, it is recommended to configure it according to the information from the official documentation on the database.

If you use a large database and dispose the appropriate computing resources, it is recommended to configure the following parameters in the `postgresql.conf` configuration file:

Minimal configuration:

```
shared_buffers = 256MB
temp_buffers = 64MB
work_mem = 16MB
```

Extended configuration:

```
shared_buffers = 1GB
temp_buffers = 128MB
work_mem = 32MB
fsync = off
synchronous_commit = off
wal_sync_method = fdatasync
commit_delay = 1000
max_locks_per_transaction = 256
max_pred_locks_per_transaction = 256
```

⚠ The `fsync = off` parameter significantly increases performance but may cause the complete loss of data in case of power failure or system crash. It is recommend to disable the `fsync` parameter only if you have a backup of the database for its full recovery.

Configuration of the `max_locks_per_transaction` parameter can be useful to ensure smooth operation at a mass appeal to the database tables, in particular, when upgrading the database to a new version.

B4. Using the MySQL DBMS

General Description

MySQL—cross-platform relational databases management system. MySQL DBMS may be used as an external DB for Dr.Web Enterprise Security Suite.

To use MySQL as an external database

1. Install the MySQL 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: in the **Dr.Web Server configuration** menu, the **Database** tab.

Installation and Supported Versions

Dr.Web Enterprise Security Suite supports the following versions of MySQL DBMS:

- MySQL—from 5.5.14 to 5.7; all versions starting from 8.0.12,
- MariaDB—10.0, 10.1, 10.2, 10.3, 10.4.

After DBMS installation, before creating a new database, it is necessary to specify the following settings in its configuration file (see your DBMS documentation for more details):

For MySQL of 5.X versions:

```
[mysqld]

innodb_large_prefix = true

innodb_file_format = barracuda

innodb_file_per_table = true

max_allowed_packet = 64M
```

For MySQL of 8.X versions:

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

If the used DBMS MariaDB has version earlier than 10.2.4, when you also must set the following in the configuration file:

```
binlog_format = mixed
```

Parameters

To adjust access to the MySQL DBMS, use the parameters described in Table B-**5**.

Table B-5. Parameters of the MySQL DBMS

Name	Default value	Description
HOST	localhost	• Database server address—when connecting to database via TCP/IP. • Path to UNIX socket file—when using UDS. If not set, Dr.Web Server tries to locate the file in one of standard mysqld directories.
PORT	3306	• Connection port number—when connecting to database via TCP/IP. • UNIX socket file name—when using UDS.
DBNAME		Database name
USER		Registration name of database user
PASSWORD	QUICK	Database user password
PRECOMPILEDCACHE	1048576	Cache size of precompiled sql operators (in bytes)
SSL	NO	Allow SSL connections only: • YES — connect to database only if SSL protocol is used, • NO — SSL protocol is not necessary to connect to database.

Appendix C. 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.conf` 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. Dr.Web 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-13.00.0-`<*build*>`-esuite-modify-ad-schema-`<*OS_version*>`.exe` utility (is included to the Dr.Web 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:

```
DrWeb_enterprise_OID "1.3.6.1.4.1" // iso.org.dod.internet.private.enterprise
DrWeb_DrWeb_OID DrWeb_enterprise_OID ".29690" // DrWeb
DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID ".1" // EnterpriseSuite
DrWeb_Alerts_OID DrWeb_EnterpriseSuite_OID ".1" // Alerts
DrWeb_Vars_OID DrWeb_EnterpriseSuite_OID ".2" // Vars
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)

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

General tags of the configuration file:

- `<enabled/>` and `<order/>`—similar to the Active Directory.
- `<server/>` specifies the LDAP server address. Multiple `<server/>` tags with different LDAP server addresses can be added, which would make a list of servers to use for authentication. A main server that is assumed to take the major load should come first, while the remaining addresses of any backup servers should come after. When administrator connects, the first available LDAP server is used. If authentication fails, it will be retried on the next server and so on, following the order in which LDAP server addresses are listed in the configuration file.
- `<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 *, # 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. LDAP/AD Authentication

Configuration File

Settings are stored in the auth-ldap-rfc4515.conf configuration file.

Configuration files with typical settings are also provided:

- auth-ldap-rfc4515-check-group.conf—configuration file template for administrators external authorization via LDAP using the simplified scheme with verification of belonging to an Active Directory group.
- auth-ldap-rfc4515-check-group-novar.conf—configuration file template for administrators external authorization via LDAP using the simplified scheme with verification of belonging to an Active Directory group and using variables.
- auth-ldap-rfc4515-simple-login.conf—configuration file template for administrators external authorization via LDAP using the simplified scheme.

General tags of the auth-ldap-rfc4515.conf configuration file:

- <server />—LDAP server definition.

Attribute	Description	Default value
base-dn	DN of an object entry relative to which the search is to be performed.	The rootDomainNamingContext attribute value of the Root DSE object
cacertfile	Root certificates files (UNIX only).	–
host	LDAP server address.	• Domain controller for the server under Windows OS.

Attribute	Description	Default value
		- `127.0.0.1` for the server under UNIX system-based OS. - Multiple `<server />` tags with different LDAP server addresses can be added. A main server that is assumed to take the major load should come first. If authentication fails, it will be retried on the next server and so on, following the specified order.
`scope`	Search scope. Allowed values: - `sub-tree`—whole sub-tree below the base DN - `one-level`—direct descendants of the base DN - `base`—base DN.	`sub-tree`
`tls`	Establish TLS on the connection to LDAP.	`no`
`ssl`	Use the LDAPS protocol at connect to LDAP.	`no`

- `<set />`—variables set by LDAP search.

Attribute	Description	Default value
`attribute`	Attribute name the value of which is assigned to a variable. Cannot be absent.	–
`filter`	RFC4515 search filter in LDAP.	–
`scope`	Search scope. Allowed values: - `sub-tree`—whole sub-tree below the base DN - `one-level`—direct descendants of the base DN - `base`—base DN.	`sub-tree`
`search`	DN of an object entry relative to which the search is to be performed.	If absent, the `base-dn` of the `<server />` tag is used.
`variable`	Variable name. Must starts with the letter and contains letters and digits only. Cannot be absent.	–

Variables can be used in values of the `add` attributes of the `<mask />` and `<expr />` tags, in value of the `value` attribute of the `<filter />` tag as the `\varname`, and also in value of the `search` attribute of the `<set />` tag. Allowed recursion level in variables is 16.

If the search returns several found objects, only the first one is used.

- `<mask />`—user name templates.

Attribute	Description
`add`	String added to a search filter using the AND operation with substitution elements.
`user`	User name mask using the DOS-like meta symbols * and #. Cannot be absent.

For example:

```
<mask user="*@#"  add="sAMAccountName=\1" />

<mask user="*\*"  add="sAMAccountName=\2" />
```

`\1` and `\2` are the links on matching masks in the `user` attribute.

- `<expr />`—user name templates using regular expressions (attributes are the same as in the `<mask />`).

For example:

```
<expr user="^(.*)@([^.,=@\s\\]+)$"  add="sAMAccountName=\1" />

<expr user="^(.*)\\(.*)"            add="sAMAccountName=\2" />
```

Correspondence between masks and regular expressions:

Mask	Regular expression
`*`	`.*`
`#`	`[^.,=@\s\\]+`

- `<filter />`—LDAP search filter.

Attribute	Description
`value`	String added to a search filter using the AND operation with substitution elements.

Filters concatenation

```
<set variable="admingrp"  filter="&amp;(objectclass=group)(cn=ESuite Admin)"
attribute="dn" />
<mask user="*\*" add="sAMAccountName=\2" />
<filter value="&amp;(objectClass=user)(memberOf=\admingrp)" />
```

If the admingrp get the "CN=ESuite Admins,OU=some name,DC=example,DC=com" value after the search, and the user input was domain\user, when the result filter is

```
"(&(sAMAccountName=user)(&(objectClass=user)(memberOf=CN=ESuite
Admins,OU=some name,DC=example,DC=com)))"
```

Example of Configuring LDAP/AD Authentication

Here is an example of typical settings for authentication using LDAP. Settings are configured in the Control Center, in the **Administration** → **Authentication** → **LDAP/AD-authentication** section (for the **Advanced settings**).

Initial parameters of administrators who must be authenticated:

- domain: dc.test.local
- Active Directory group: DrWeb_Admins

Control Center settings:

Setting name		**Value**
Server type		Microsoft Active Directory
Server address		dc.test.local
Login templates of users to be authenticated	Account mask	test* or *@test.local
	Login	\1
Membership of users to be authenticated	Name	DrWeb_Admins
	Type	group

C4. Depended Permissions Sections

Table C-1. The list of administrative rights and their features

Code	**Permission**	**Description**	**Control Center section**
Manage groups of stations			
1*	**View groups of stations properties**	The list of user groups which administrator sees in the anti-virus network. All system groups are also	Anti-virus Network

Code	Permission	Description	Control Center section
		displayed in the anti-virus network tree, but only stations from the specified group list are available inside.	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.	
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 Pages from the **Configuration** section
4	**Edit groups of stations configuration**	Same as permission 3, but editing is permitted. Must contain groups from the list of permission 3.	
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.	Anti-virus Network
9	**Delete stations**	The list of user groups that are primary for stations which administrator can	

Code	Permission	Description	Control Center section
		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.	
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. The permission allows to create a task in the Dr.Web 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. Must contain groups from the list of permission 1.	Anti-virus Network pages from the **Statistics** section
23	**Edit licensing**	The list of user groups for which administrator can add/change/remove	

Code	Permission	Description	Control Center section
		a license key. These groups must be a primary for the stations. Must contain groups from the list of permission 1.	
Manage administrators			
25	**Create administrators, administrative groups**	The corresponding icon in the toolbar is hidden either.	Administration → Configuration → Administrators
26	**Edit administrators accounts**	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. Administrator can edit administrative accounts from the specified groups. At this, the corresponding icon in the toolbar become available.	
27	**Delete administrators accounts**	Same as permission 26.	
28	**View properties and configuration of administrative groups**	Including administrators in groups and subgroups. Administrator is able to select only from a subgroup of own parent group.	
39	**Display the "Newbies" administrative group**	Allow administrator to view the pre-installed **Newbies** group in the administrators tree. If administrator has not got permissions for viewing the group **Newbies**, and administrator is in this group, then administrator will see only own account.	
29	**Edit properties and configuration of administrative groups**	Including administrators in groups and subgroups.	

Code	Permission	Description	Control Center section
		Administrator is able to select only from a subgroup of own parent group. 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.	
Additional			
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
16	**Run Network scanner**	If the permission is denied, the network installation for the /esuite/network/index.ds is not available.	Anti-virus Network Administration → Network scanner
17	**Approve newbies**	The groups list from permission 8 is available. This permission cannot be granted if an administrator is allowed to manage only several groups but not all anti-virus network objects. I.e., for the permission 1 (**View groups of stations properties**) the set of groups is specified.	Anti-virus Network
18	**View Dr.Web Server schedule**	The **Tasks execution log** table viewing. If permissions 12 and 18 are denied, the viewing of the Dr.Web Server schedule page is forbidden.	Administration → Configuration → Dr.Web Server Task Scheduler Administration → Statistics → Task execution log

Code	Permission	Description	Control Center section
		If permission 12 is allowed but 18 is denied, when viewing statistics, the schedule is available. The task for sending reports to an administrator is displayed depending on the presence of permission 12 and the **Periodic report** notification, even if permission 18 is denied.	
19	**Edit Dr.Web Server schedule**		Administration → Configuration → Dr.Web Server Task Scheduler
20	**View Dr.Web 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 Administration → Repository → Repository content Administration → Logs → Log of repository updates Administration → Configuration → User hooks Administration → Dr.Web Server → Versions list
21	**Edit Dr.Web Server configuration and repository configuration**		

Code	Permission	Description	Control Center section
22	**View license information**		Administration → Administration → License Manager
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**		Neighbors
32	**Edit neighborhood connections**		Neighbors
33	**Use additional features**	Limits assess to all subsections of **Additional features** section except the **Utilities** subsection which is always available.	Administration → Additional features
34	**Update repository**	Update Dr.Web Server repository from GUS.	The **Update repository** button in the **Repository state** section
42	**Edit own settings**	Permission to edit settings of own administrative account	Administration → Configuration → Administrators

* 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 this 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. 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 sens are used:

- email notifications,
- notifications via the Web Console,
- notifications via SNMP,
- notifications via the Agent protocol,
- push notifications.

Depending on the notification sens 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	-

Parameter	Description	Default value
HOST	SMTP server address	127.0.0.1
PORT	SMTP server port number	• 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	Encrypt data transfer. At this, switching to secured connection is performed by using the STARTTLS command. The 25 port is used by default for the connection.	yes
SSL	Encrypt data transfer. At this, a new secured TLS connection is established. The 465 port is used by default for the connection.	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 Web console

Parameter	Description	Default value
TO	UUID of administrators, to which this notification will be send	-

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

Table D-4. Notifications via SNMP

Parameter	Description	Default value
TO	SNMP receiving entity, e.g., IP address	-
DOMAIN	Domain	• 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-5. 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-6. 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	-

D2. The Parameters of Notification Templates

The text for messages is generated by a Dr.Web 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.
>
> The Windows Vista OS and later versions 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 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.

  The number of substitution pairs are not limited.
- {<VAR>/<original1>/<replace1[{<SUB_VAR>}]>[/<original2>/<replace2>]}—similarly to the above described replaces to the specified values but the <SUB_VAR> nested variable is used. Actions with nested variables are the same as the actions with parent variables.

  Nesting level for recursive substitutions is not limited.
- {<VAR>/<original1>/<replace1>/<original2>/<replace2>/*/<replace3>}—similarly to the above described replaces to the specified values but also the value from <replace3> can be substituted, if none of the listed original values match. Also, if either <original1>, or <original2> have not been found in <VAR>, all values will be replaced with the <replace3>.

Table D-7. 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

Variable	Value	Expression	Result
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 Dr.Web 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.BRANCH`—system version (Dr.Web Server and Agents),
- `SYS.BUILD`—Dr.Web Server build date,
- `SYS.DATE`—current system date,
- `SYS.DATETIME`—current system date and time,
- `SYS.HOST`—Dr.Web Server DNS name,
- `SYS.MACHINE`—network address of a computer with Dr.Web Server installed,
- `SYS.OS`—operating system name of a computer with Dr.Web Server installed,
- `SYS.PLATFORM`—Server platform,
- `SYS.PLATFORM.SHORT`—short variant of `SYS.PLATFORM`,
- `SYS.SERVER`—product name (Dr.Web Server),
- `SYS.TIME`—current system time,
- `SYS.VERSION`—Dr.Web Server version.

Common Variables for Stations

- `GEN.LoginTime`—station login time,
- `GEN.StationAddress`—station address,
- `GEN.StationDescription`—station description,

- GEN.StationID—station unique identifier,
- GEN.StationLDAPDN—distinguished name of a station under Windows OS. Relevant for stations included into ADS/LDAP domain,
- GEN.StationMAC—stations MAC address,
- GEN.StationName—station name,
- GEN.StationPrimaryGroupID—identifier of the station primary group,
- GEN.StationPrimaryGroupName—name of the station primary group,
- GEN.StationSID—security identifier of a station.

Common Variables for Repository

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

Notification Parameters and Variables by Types

Administrators

Administrator authorization failed

Parameter	Value	
Notification sending reason	Sent on error of administrator authorization in the Control Center. The reason of authorization failure is given in the notification text.	
Additional configuration	Not required.	
Variables	MSG.Login	login
	MSG.Address	Control Center network address
	MSG.LoginErrorCode	numeric error code

Unknown administrator

Parameter	Value
Notification sending reason	Sent on attempt of authorization in the Control Center by administrator with unknown login.

Parameter	Value	
Additional configuration	Not required.	
Variables	`MSG.Login`	login
	`MSG.Address`	network address of Dr.Web Security Control Center

Installations

For messages of this group, you can also use common variables for stations given above.

Installation on station failed

Parameter	Value	
Notification sending reason	Sent if an error occurred during the Agent installation on a station. The error reason is given in the notification text.	
Additional configuration	Not required.	
Variables	`MSG.Error`	error message

Installation on station successfully completed

Parameter	Value
Notification sending reason	Sent on succeeded Agent installation on a station.
Additional configuration	Not required.
Variables	Absent.

Licenses

License key automatically updated

Parameter	Value
Notification sending reason	Sent if a license key has been automatically updated. At this, a new key has been successfully downloaded and propagated on all objects of an old license key.
Additional configuration	For detailed information on automatic license update, refer the

Parameter	Value	
	Administrator Manual, p. Automatic Licenses Update.	
Variables	`MSG.KeyId`	Identifier of an old license key
	`MSG.KeyName`	Name of an old license key
	`MSG.NewKeyId`	Identifier of a new license key
	`MSG.NewKeyName`	Name of a new license key

License key blocked

Parameter	Value	
Notification sending reason	Sent if during the update from Dr.Web Global Update System, information on the license key blocking has been received. This key can no longer be used.	
Additional configuration	To get detailed information on blocking reason, please contact the technical support service.	
Variables	`MSG.KeyId`	ID of a license key
	`MSG.KeyName`	Name of a user of a license key

License key cannot be automatically updated

Parameter	Value	
Notification sending reason	Sent if a license key cannot be automatically updated, because the compound of licensed components differs in the current and the new keys. At this, a new key successfully downloaded but not propagated on all objects of an old license key. You must replace the license key manually.	
Additional configuration	For detailed information on automatic license update, refer the **Administrator Manual**, p. Automatic Licenses Update.	
Variables	`MSG.ExpirationDate`	date of license expiration
	`MSG.Expired`	• 1—the term has expired • 0—the term has not expired
	`MSG.KeyDifference`	The reason why automatic replacement is impossible: • the compound of licensed

Parameter	Value	
		components differs in the current and the new license keys • the new license key has fewer licenses than the current license key
	`MSG.KeyId`	Identifier of an old license key
	`MSG.KeyName`	Name of an old license key
	`MSG.NewKeyId`	Identifier of a new license key
	`MSG.NewKeyName`	Name of a new license key

License key expiration

Parameter	Value	
Notification sending reason	Sent if the license key is about to expire, and automatic license update is not available.	
Additional configuration	Not required.	
Variables	`MSG.ExpirationDate`	date of license expiration
	`MSG.Expired`	• 1—the term has expired • 0—the term has not expired
	`MSG.KeyId`	Identifier of a license key
	`MSG.KeyName`	Name of a license key

License limitation on a number of online stations is reached

Parameter	Value
Notification sending reason	Sent if during connection of a station to Dr.Web 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. At this, a new station cannot register on Dr.Web Server.
Additional configuration	Not required.

Parameter	Value	
Variables	`MSG.ID`	station UUID
	`MSG.StationName`	station name
	Common variables for stations given above are also available.	

Licenses donation has expired

Parameter	Value	
Notification sending reason	Sent if the period of licenses donation to neighbor Dr.Web Servers from the license key of this Dr.Web Server has expired.	
Additional configuration	The period of licenses donation to neighbor Dr.Web Servers is specified in the **Administration** → **Dr.Web Server configuration** → **Licenses** section.	
Variables	`MSG.ObjId`	license key ID
	`MSG.Server`	the neighbor Dr.Web Server name

Limitation on a number of donated licenses is reached

Parameter	Value	
Notification sending reason	Sent if the number of requested licenses for donation to neighbor Dr.Web Servers exceeds the number of licenses that are available in the license key.	
Additional configuration	Not required.	
Variables	`MSG.ObjId`	license key ID

Limitation on a number of licenses in the license key

Parameter	Value	
Notification sending reason	Sent if during the Dr.Web 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.	
Additional configuration	Not required.	
Variables	`MSG.KeyId`	ID of a license key

Parameter	Value	
	`MSG.KeyName`	license key user name
	`MSG.Licensed`	number of allowed licenses
	`MSG.LicenseLimit`	licenses state: • 1—number of free licenses in the license key is close to the end • 2—number of free licenses in the license key has ended • 3—the license key has been assigned to more objects than allowed in this key.
	`MSG.Licensed`	number of objects to which the key has been assigned
	`MSG.Total`	number of licenses in the key

Number of stations in the group is close to the license limit

Parameter	Value	
Notification sending reason	Sent if the number of stations in the group is closing to the license limitation in the key assigned to this group.	
Additional configuration	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.	
Variables	`MSG.Free`	number of free licenses left
	`MSG.Licensed`	number of stations using licenses of this group
	`MSG.Total`	Total number of licenses in all keys assigned to the group. Please note: license keys of the group can also be assigned to other licensing objects.

Parameter	Value	
	`GEN.StationPrimaryGroupID`	primary group ID
	`GEN.StationPrimaryGroupName`	primary group name

Newbies

For messages of this group, you can also use common variables for stations given above.

Station automatically rejected

Parameter	Value
Notification sending reason	Sent if a new station requested a connection to Dr.Web Server and has been rejected by Dr.Web Server automatically.
Additional configuration	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.
Variables	Absent.

Station is waiting for approval

Parameter	Value
Notification sending reason	Sent if a new station requested a connection to Dr.Web Server and administrator must approve or reject the station manually.
Additional configuration	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.
Variables	Absent.

Station rejected by administrator

Parameter	Value
Notification sending reason	Sent if a new station requested a connection to Dr.Web Server and has been rejected by administrator manually.
Additional configuration	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

Parameter	Value	
	administrator selected the **Anti-virus Network** → **Unapproved stations** → **Reject selected stations** option for this station.	
Variables	`MSG.AdminAddress`	network address of the Control Center
	`MSG.AdminName`	administrator name

Other

Epidemic in the network

Parameter	Value	
Notification sending reason	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.	
Additional configuration	To sent epidemic notifications, you must set the **Track epidemic** flag in the **Administration** → **Dr.Web Server configuration** → **Statistics** section. Parameters on epidemic detection are set in the same section.	
Variables	`MSG.Infected`	total number of detected threats
	`MSG.Virus`	the most common threats

Large number of abnormally terminated connections detected

Parameter	Value	
Notification sending reason	Sent on a large number of abnormally terminated connections with clients: stations, Agent installers, neighbor Dr.Web Servers, Proxy Servers.	
Additional configuration	To be able to sent notifications on multiple abnormally terminated connections, you must set the **Abnormally terminated connections** flag in the **Administration** → **Dr.Web Server configuration** → **Statistics** section and configure corresponding parameters in the same section.	
Variables	`MSG.Total`	number of terminated connections

Parameter	Value	
	`MSG.AddrsCount`	number of addresses that were disconnected

Large number of blocks by the Application Control detected

Parameter	Value	
Notification sending reason	Sent on a large number of blocked applications at stations by the Application Control component.	
Additional configuration	To be able to sent notifications on multiple blocked applications, you must set the **Multiple blockings by Application Control** flag in the **Administration → Dr.Web Server configuration → Statistics** section and configure corresponding parameters in the same section.	
Variables	`MSG.Total`	total number of blocks
	`MSG.Profile`	most common profiles according to which the block was made

Neighbor server has not connected for a long time

Parameter	Value	
Notification sending reason	Sent according to the task in the Dr.Web Server schedule. Contains information that the neighbor Dr.Web Server has not connected to this Dr.Web Server for a long time. The date of last connection is given in the notification text.	
Additional configuration	The time period during which the neighbor Dr.Web 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 Dr.Web Server schedule configured in the **Administration → Dr.Web Server Task Schedule**.	
Variables	`MSG.LastDisconnectTime`	the time when Dr.Web Server has been connected at the last time
	`MSG.StationName`	the neighbor Dr.Web Server name

Dr.Web Server log rotation error

Parameter	Value	
Notification sending reason	Sent if an error occurred during rotation of the Dr.Web Server operation log. The reason of log rotation error is given in the notification text.	
Additional configuration	Not required.	
Variables	`MSG.Error`	message text

Dr.Web Server log write error

Parameter	Value	
Notification sending reason	Sent when an error occurred during writing an information into the Dr.Web Server operation log. The reason of log write error is given in the notification text.	
Additional configuration	Not required.	
Variables	`MSG.Error`	message text

Statistic report

Parameter	Value	
Notification sending reason	Sent after generation of a periodic report according to the task in the Dr.Web Server schedule. Also, notification contains the path for downloading the report file.	
Additional configuration	The report is generated according to the **Statistic reports** task in the Dr.Web Server schedule configured in the **Administration** → **Dr.Web Server Task Schedule**.	
Variables	`MSG.Attachment`	path to the report
	`MSG.AttachmentType`	MIME type
	`GEN.File`	report file name

Summary report of Preventive protection

Parameter	Value	
Notification sending reason	Sent at receiving a lot of reports from the Preventive protection component on the network stations.	
Additional configuration	To send a single notification on the Preventive protection report, you must set the **Group reports of Preventive protection** flag in the **Administration** → **Dr.Web Server configuration** → **Statistics** section. Parameters on reports grouping are set in the same section.	
Variables	`MSG.AutoBlockedActCount`	number of processes with suspicious activity that were blocked automatically
	`MSG.AutoBlockedProc`	processes with suspicious activity that were blocked automatically
	`MSG.HipsType`	protected object type
	`MSG.IsShellGuard`	dividing on types of the Preventive protection reactions at automatic blocking: • blocking of unauthorized code • check the access to the protected objects
	`MSG.ShellGuardType`	the most common reason of a blocking of unauthorized code execution at automatic event blocking
	`MSG.Total`	total number of Preventive protection events detected on the network
	`MSG.UserAllowedActCount`	number of processes with suspicious activity that were allowed by user
	`MSG.UserAllowedHipsType`	type of the most common protected objects access to which was allowed by user
	`MSG.UserAllowedIsShellGuard`	dividing on types of the Preventive protection reactions when the access was allowed by

Parameter	Value	
		user: • blocking of unauthorized code • check the access to the protected objects
	`MSG.UserAllowedProc`	processes with suspicious activity that were allowed by user
	`MSG.UserAllowedShellGuard`	the most common reason of a blocking of unauthorized code execution which was allowed by user
	`MSG.UserBlockedActCount`	number of processes with suspicious activity that were blocked by user
	`MSG.UserBlockedHipsType`	type of the most common protected objects access to which was blocked by user
	`MSG.UserBlockedIsShellGuard`	dividing on types of the Preventive protection reactions when the access was blocked by user: • blocking of unauthorized code • check the access to the protected objects
	`MSG.UserBlockedProc`	processes with suspicious activity that were blocked by user
	`MSG.UserBlockedShellGuard`	the most common reason of a blocking of unauthorized code execution which was blocked by user

Repository

For messages of this group, you can also use common variables for repository given above.

Not enough free space on disk

Parameter	Value	
Notification sending reason	Sent if on a disk where the Dr.Web Server `var` folder with variable data located, is running out of space.	
Additional configuration	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.	
Variables	Common variables for repository given above are not available.	
	`MSG.FreeInodes`	the number of free inodes file descriptors (has the meaning only for some UNIX system-based OS)
	`MSG.FreeSpace`	free space in bytes
	`MSG.Path`	the path to the folder with low free space
	`MSG.RequiredInodes`	number of free inodes required for operation (has the meaning only for some UNIX system-based OS)
	`MSG.RequiredSpace`	free space required for operation

Repository cannot be updated

Parameter	Value	
Notification sending reason	Sent if during update of repository or repository product from the GUS, an error has occurred. Reason of the update error and also the name of the product at product update error, are given in the notification text.	
Additional configuration	Not required.	
Variables	`MSG.Error`	error message
	`MSG.ExtendedError`	detailed description of an error

Repository product is up-to-date

Parameter	Value
Notification sending reason	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.
Additional configuration	Not required.
Variables	Absent.

> The variables of the **Repository product is up-to-date** 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.

Repository product is updated

Parameter	Value	
Notification sending reason	Sent when repository update from the GUS successfully completed.	
Additional configuration	Not required.	
Variables	`MSG.Added`	list of added files (each name in a separate line)
	`MSG.AddedCount`	number of added files
	`MSG.Deleted`	list of deleted files (each name in a separate line)
	`MSG.DeletedCount`	number of deleted files
	`MSG.Replaced`	list of replaced files (each name in a separate line)
	`MSG.ReplacedCount`	number of replaced files

Repository update already running

Parameter	Value
Notification sending reason	Sent if during the Dr.Web Server update, the other update was started.

Parameter	Value
Additional configuration	Not required.
Variables	Absent.

Update of repository product is frozen

Parameter	Value
Notification sending reason	Sent if the repository product was frozen by administrator. At this, update of this product from the GUS is not performed.
Additional configuration	You can manage repository products including their frozen and unfrozen states in the **Administration → Detailed repository configuration** section.
Variables	Absent.

Update of repository product is started

Parameter	Value
Notification sending reason	Sent if during repository updates check, it was detected that for requested products the update is required. At this, the update from the GUS is launched.
Additional configuration	Not required.
Variables	Absent.

Stations

For messages of this group, you can also use common variables for stations given above.

In multiserver network, it is possible to receive notifications about events on stations of neighbor Dr.Web Servers. You can enable this option when configuring neighbor Dr.Web Server connections (see **Administrator Manual**, the Setting Connections between Several Dr.Web Servers section).

The following notifications are available to receive on event on the neighbor Dr.Web Server: **Security threat detected**, **Report of Preventive protection**, **Scan error**, **Scan statistics**.

Application Control blocked the process

Parameter	Value	
Notification sending reason	Sent if an application was blocked at station by the Application Control component.	
Additional configuration	Not required.	
Variables	`MSG.AppCtlAction`	applied action: • 0—unknown, • 2—blocked • 3—blocked (not found in the trusted applications list) • 5—blocked by deny rules • 7—blocked by policies settings.
	`MSG.AppCtlType`	event type: • 0—unknown • 1—process launch • 2—host process launch • 3—script interpreter launch • 4—module load • 5—driver load • 6—MSI setup launch • 7—new executable file dropped on disk • 8—executable file modified on disk.
	`MSG.Path`	path to the blocked process
	`MSG.Profile`	name of the profile according to which the block was made
	`MSG.Rule`	name of the rule according to which the block was made
	`MSG.SHA256`	blocked process hash (SHA-256)
	`MSG.StationTime`	station time when the process was blocked
	`MSG.Target`	path to the blocked script in case

Parameter	Value	
		of host process
	`MSG.TargetSHA256`	hash the blocked script in case of host process (SHA-256)
	`MSG.TestMode`	whether the test mode is on
	`MSG.User`	user on behalf of which the blocked object was launched

Application Control blocked the process from the known hashes of threats list

Parameter	Value	
Notification sending reason	Sent if an application from the known hashes of threats was blocked at station by the Application Control component.	
Additional configuration	Notification on detection by the list of known hashes is possible only if the usage of bulletins of known threat hashes is licensed (the license in at least one of the license keys used by Dr.Web Server is sufficient). You can check the license in the information on a license key that can be found in the **License Manager** section, the **Allowed lists of hash bulletins** parameter (If the feature is not licensed, this parameter is absent).	
Variables	`MSG.AppCtlAction`	applied action: • 0—unknown, • 2—blocked • 3—blocked (not found in the trusted applications list) • 5—blocked by deny rules • 7—blocked by policies settings.
	`MSG.AppCtlType`	event type: • 0—unknown • 1—process launch • 2—host process launch • 3—script interpreter launch • 4—module load • 5—driver load • 6—MSI setup launch

Parameter	Value	
		• 7—new executable file dropped on disk • 8—executable file modified on disk.
	`MSG.Document`	bulletin containing the hash
	`MSG.Path`	path to the blocked process
	`MSG.Profile`	name of the profile according to which the block was made
	`MSG.Rule`	name of the rule according to which the block was made
	`MSG.SHA256`	blocked process hash (SHA-256)
	`MSG.StationTime`	station time when the process was blocked
	`MSG.Target`	path to the blocked script in case of host process
	`MSG.TargetSHA256`	hash the blocked script in case of host process (SHA-256)
	`MSG.TestMode`	whether the test mode is on
	`MSG.User`	user on behalf of which the blocked object was launched

Cannot create the station account

Parameter	Value	
Notification sending reason	Sent if a new stations account cannot be created on Dr.Web Server. Error details are given in the Dr.Web Server log file.	
Additional configuration	Not required.	
Variables	`MSG.ID`	station UUID
	`MSG.StationName`	station name

Connection terminated abnormally

Parameter	Value	
Notification sending reason	Sent on abnormal termination of a connection with a client: station, Agent installer, neighbor Dr.Web Server, Proxy Server.	
Additional configuration	To be able to sent notifications on abnormally terminated connections, you must set the **Abnormally terminated connections** flag in the **Administration** → **Dr.Web Server configuration** → **Statistics** section and configure corresponding parameters in the same section.	
Variables	`MSG.Total`	number of terminated connections
	`MSG.Type`	client type

Critical error of station update

Parameter	Value	
Notification sending reason	Sent if a notification received from a station reports an error during update of anti-virus components from Dr.Web Server.	
Additional configuration	Not required.	
Variables	`MSG.Product`	updated product
	`MSG.ServerTime`	local time of receipt of a message by Dr.Web Server

Device blocked

Parameter	Value	
Notification sending reason	Sent if a notification received from a station reports that a connected to the station device has been blocked by Dr.Web anti-virus component.	
Additional configuration	Not required.	
Variables	`MSG.Capabilities`	device characteristics
	`MSG.Class`	device class (the name of a parent group)

Parameter	Value	
	`MSG.Description`	device description
	`MSG.FriendlyName`	user friendly name of the device
	`MSG.InstanceId`	identifier of a device instance
	`MSG.User`	user name

Report of Preventive protection

Parameter	Value	
Notification sending reason	Sent at receiving the report from the Preventive protection component from a station of this or neighbor Dr.Web Server.	
Additional configuration	Not required.	
Variables	`MSG.AdminName`	administrator who initiated the action on a suspicious process
	`MSG.Denied`	action on a suspicious process: • denied • allowed
	`MSG.HipsType`	protected object type
	`MSG.IsShellGuard`	dividing on types of the Preventive protection reactions: • blocking of unauthorized code • check the access to the protected objects
	`MSG.Path`	path to the process with suspicious activity
	`MSG.Pid`	identifier of the process with suspicious activity
	`MSG.ShellGuardType`	reason of execution of unauthorized code blocking
	`MSG.StationTime`	time of event occurrence on a station
	`MSG.Target`	path to the protected object to which the access attempt was

Parameter	Value	
		made
	MSG.Total	number of denials in case of automatic reaction of the Preventive protection
	MSG.User	user who launched the suspicious process
	MSG.UserAction	initiator of the action on a suspicious process • user • automatic reaction of the Preventive protection
	GEN.ServerRecvLinkID	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	GEN.ServerRecvLinkName	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	GEN.ServerOriginatorID	UUID of the Dr.Web Server to which the station is connected from which the Preventive protection report was received
	GEN.ServerOriginatorName	the name of the Dr.Web Server to which the station is connected from which the Preventive protection report was received

Report of Preventive protection on threat detection by known hashes of threats

Parameter	Value
Notification sending reason	Sent at receiving the report from the Preventive protection

Parameter	Value	
	component from a station of this or neighbor Dr.Web Server at threat detection from the list of known hashes of threats.	
Additional configuration	Notification on detection by the list of known hashes is possible only if the usage of bulletins of known threat hashes is licensed (the license in at least one of the license keys used by Dr.Web Server is sufficient). You can check the license in the information on a license key that can be found in the **License Manager** section, the **Allowed lists of hash bulletins** parameter (If the feature is not licensed, this parameter is absent).	
Variables	`MSG.AdminName`	administrator who initiated the action on a suspicious process
	`MSG.Denied`	action on a suspicious process: • denied • allowed
	`MSG.Document`	bulletin containing the hash of detected threat
	`MSG.HipsType`	protected object type
	`MSG.IsShellGuard`	dividing on types of the Preventive protection reactions: • blocking of unauthorized code • check the access to the protected objects
	`MSG.Path`	path to the process with suspicious activity
	`MSG.Pid`	identifier of the process with suspicious activity
	`MSG.SHA1`	SHA-1 hash of detected object
	`MSG.SHA256`	SHA-256 hash of detected object
	`MSG.ShellGuardType`	reason of execution of unauthorized code blocking
	`MSG.StationTime`	time of event occurrence on a station

Parameter	Value	
	`MSG.Target`	path to the protected object to which the access attempt was made
	`MSG.Total`	number of denials in case of automatic reaction of the Preventive protection
	`MSG.User`	user who launched the suspicious process
	`MSG.UserAction`	initiator of the action on a suspicious process • user • automatic reaction of the Preventive protection
	`GEN.ServerRecvLinkID`	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerRecvLinkName`	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerOriginatorID`	UUID of the Dr.Web Server to which the station is connected from which the Preventive protection report was received
	`GEN.ServerOriginatorName`	the name of Dr.Web Server to which the station is connected from which the Preventive protection report was received

Scan error

Parameter	Value	
Notification sending reason	Sent if a notification received from a station reports an error during scanning.	
Additional configuration	Not required.	
Variables	`MSG.Component`	component name
	`MSG.Error`	error message
	`MSG.ObjectName`	object name
	`MSG.ObjectOwner`	object owner
	`MSG.RunBy`	component is launched by this user
	`MSG.ServerTime`	event receipt time, GMT
	`GEN.ServerRecvLinkID`	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerRecvLinkName`	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerOriginatorID`	UUID of the Dr.Web Server to which the station is connected from which the Preventive protection report was received
	`GEN.ServerOriginatorName`	the name of the Dr.Web Server to which the station is connected from which the Preventive protection was received

Scan error at threat detection by known hashes of threats

Parameter	Value	
Notification sending reason	Sent if scan error occurred at threat detection from the list of known hashes of threats.	
Additional configuration	Notification on detection by the list of known hashes is possible only if the usage of bulletins of known threat hashes is licensed (the license in at least one of the license keys used by Dr.Web Server is sufficient). You can check the license in the information on a license key that can be found in the **License Manager** section, the **Allowed lists of hash bulletins** parameter (If the feature is not licensed, this parameter is absent).	
Variables	`MSG.Component`	component name
	`MSG.Document`	bulletin containing the hash of detected threat
	`MSG.Error`	error message
	`MSG.ObjectName`	object name
	`MSG.ObjectOwner`	object owner
	`MSG.RunBy`	component is launched by this user
	`MSG.SHA1`	SHA-1 hash of detected object
	`MSG.SHA256`	SHA-256 hash of detected object
	`MSG.ServerTime`	event receipt time, GMT
	`GEN.ServerRecvLinkID`	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerRecvLinkName`	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was

Parameter	Value	
		received about stations connected to this Dr.Web Server)
	`GEN.ServerOriginatorID`	UUID of the Dr.Web Server to which the station is connected from which the Preventive protection report was received
	`GEN.ServerOriginatorName`	the name of the Dr.Web Server to which the station is connected from which the Preventive protection report was received

Scan statistics

Parameter	Value	
Notification sending reason	Sent if a notification received from a station reports a scan completion. Administrative notification also contains brief scan statistic.	
Additional configuration	Not required.	
Variables	`MSG.Component`	component name
	`MSG.Cured`	number of cured objects
	`MSG.DeletedObjs`	number of deleted objects
	`MSG.Errors`	number of scan errors
	`MSG.Infected`	number of infected objects
	`MSG.Locked`	number of blocked objects
	`MSG.Modifications`	number of objects infected with known modifications of viruses
	`MSG.Moved`	number of moved objects
	`MSG.Renamed`	number of renamed objects
	`MSG.RunBy`	component is launched by this user
	`MSG.Scanned`	number of scanned objects

Parameter	Value	
	`MSG.ServerTime`	event receipt time, GMT
	`MSG.Speed`	processing speed in KB/s
	`MSG.Suspicious`	number of suspicious objects
	`MSG.VirusActivity`	number of detected viruses
	`GEN.ServerRecvLinkID`	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerRecvLinkName`	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerOriginatorID`	UUID of the Dr.Web Server to which the station is connected from which the Preventive protection report was received
	`GEN.ServerOriginatorName`	the name of the Dr.Web Server to which the station is connected from which the Preventive protection report was received

Security threat detected

Parameter	Value	
Notification sending reason	Sent if a notification received from a station reports the threat detection. Administrative notification also contains detailed information on detected threats.	
Additional configuration	Not required.	
Variables	`MSG.Action`	action upon a detection
	`MSG.Component`	component name

Parameter	Value	
	`MSG.InfectionType`	threat type
	`MSG.ObjectName`	infected object name
	`MSG.ObjectOwner`	infected object owner
	`MSG.RunBy`	component is launched by this user
	`MSG.ServerTime`	event receipt time, GMT
	`MSG.Virus`	threat name
	`GEN.ServerRecvLinkID`	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerRecvLinkName`	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerOriginatorID`	UUID of Dr.Web Server to which the station is connected from which the Preventive protection report was received
	`GEN.ServerOriginatorName`	the name of Dr.Web Server to which the station is connected from which the Preventive protection report was received

Security threat detected by known hashes of threats

Parameter	Value
Notification sending reason	Sent if a notification received from a station reports the threat detection from the list of known hashes of threats. Administrative notification also contains detailed information on detected threats.

Parameter	Value	
Additional configuration	Notification on detection by the list of known hashes is possible only if the usage of bulletins of known threat hashes is licensed (the license in at least one of the license keys used by Dr.Web Server is sufficient). You can check the license in the information on a license key that can be found in the **License Manager** section, the **Allowed lists of hash bulletins** parameter (If the feature is not licensed, this parameter is absent).	
Variables	`MSG.Action`	action upon a detection
	`MSG.Component`	component name
	`MSG.Document`	bulletin containing the hash of detected threat
	`MSG.InfectionType`	threat type
	`MSG.ObjectName`	infected object name
	`MSG.ObjectOwner`	infected object owner
	`MSG.RunBy`	component is launched by this user
	`MSG.SHA1`	SHA-1 hash of detected object
	`MSG.SHA256`	SHA-256 hash of detected object
	`MSG.ServerTime`	event receipt time, GMT
	`MSG.Virus`	threat name
	`GEN.ServerRecvLinkID`	UUID of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)
	`GEN.ServerRecvLinkName`	the name of the last neighbor Dr.Web Server from which the Preventive protection report on connected stations was received (empty value if the report was received about stations connected to this Dr.Web Server)

Parameter	Value	
	GEN.ServerOriginatorID	UUID of the Dr.Web Server to which the station is connected from which the Preventive protection report was received
	GEN.ServerOriginatorName	the name of the Dr.Web Server to which the station is connected from which the Preventive protection report was received

Station already logged in

Parameter	Value	
Notification sending reason	Send on attempt to connect to Dr.Web Server of a station with identifier which matches the identifier of a station already connected to this Dr.Web Server.	
Additional configuration	Not required.	
Variables	MSG.ID	station UUID
	MSG.Server	ID of the Dr.Web Server at which the station is registered
	MSG.StationName	station name

Station approved by administrator

Parameter	Value	
Notification sending reason	Sent if a new station requested a connection to Dr.Web Server and has been approved by administrator manually.	
Additional configuration	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.	
Variables	MSG.AdminAddress	network address of the Control Center
	MSG.AdminName	administrator name

Station authorization failed

Parameter	Value	
Notification sending reason	Sent if a station provided incorrect credentials when trying to connect to Dr.Web Server. Further actions that depend on a stations approval policy, are also given in the notification.	
Additional configuration	Stations approval policy is set in the **Newbies registration mode** option of the **Administration → Dr.Web Server configuration → General** section.	
Variables	`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
	`MSG.StationName`	station name

Station automatically approved

Parameter	Value
Notification sending reason	Sent if a new station requested a connection to Dr.Web Server and has been approved by Dr.Web Server automatically.
Additional configuration	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.
Variables	Absent.

Station has not connected to Dr.Web Server for a long time

Parameter	Value
Notification sending reason	Sent according to the task in the Dr.Web Server schedule. Contains information that the station has not connected to this Dr.Web Server for a long time. The date of last connection is given in the notification text.
Additional configuration	The time period during which the station should not get connected

Parameter	Value	
	to send the notification, is set in the **Station has not connected for a long time** task of the Dr.Web Server schedule configured in the **Administration → Dr.Web Server Task Schedule**.	
Variables	Common variables for stations given above are not available.	
	`MSG.DaysAgo`	number of days since the last connection to Dr.Web Server
	`MSG.LastSeenFrom`	address of the station at the last connection to Dr.Web Server
	`MSG.StationDescription`	station description
	`MSG.StationID`	station UUID
	`MSG.StationMAC`	station MAC address
	`MSG.StationName`	station name
	`MSG.StationSID`	station security identifier

Station reboot required

Parameter	Value	
Notification sending reason	Sent if a station reboot is required for one of the following reasons: • to complete the cure • to apply the updates • to change the state of hardware virtualization • to complete the cure and apply the updates • to complete the cure and change the state of hardware virtualization • to apply the updates and change the state of hardware virtualization • to complete the cure, apply the updates and change the state of hardware virtualization.	
Additional configuration	Not required.	
Variables	`MSG.Reason`	reboot reason the list of possible reboot reasons is given in the predefined template

Station reboot required to apply updates

Parameter	Value	
Notification sending reason	Sent if a notification received from a station reports that the product has been installed or updated, and the station restart is required.	
Additional configuration	Not required.	
Variables	`MSG.Product`	updated product
	`MSG.ServerTime`	local time of receipt of a message by Dr.Web Server

Unknown station

Parameter	Value	
Notification sending reason	Sent if a new station requested a connection to Dr.Web Server, but was not allowed to review for approval or rejection of the registration.	
Additional configuration	Not required.	
Variables	`MSG.ID`	UUID of unknown station
	`MSG.Rejected`	values: • `rejected`—access to a station is denied • `newbie`—there was an attempt to assign the "newbie" status to a station
	`MSG.StationName`	station name

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.

The following obsolete addresses format is also allowed:

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

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.

When you specify an address of Dr.Web Server or the Agent, you can set the version of the protocol to use. The following variants are available:

- *<protocol>*`://`*<interface>*`:`*<port-number>* – use IPv4 and IPv6.
- *<protocol>*`://(`*<interface>*`):`*<port-number>* – use IPv4 only.
- *<protocol>*`://[`*<interface>*`]:`*<port-number>* – use IPv6 only.

For Example:

1. `tcp://127.0.0.1:2193`

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

2. `tcp://(examle.com):2193`

means a TCP protocol, port `2193` on an IPv4 interface `examle.com`.

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

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

4. `localhost:2193`

   the same.

5. `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`.

6. `tcp://`

   TCP protocol, default port.

Connection-Oriented Protocol

<protocol>/*<socket-address>*

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

Datagram-Oriented Protocol

<protocol>://*<endpoint-socket-address>*[-*<interface>*]

For Example:

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.

UDS Addresses

- Connection-oriented protocol:

  `unx://`*<file_name>*

- Datagram-oriented protocol:

  `udx://`*<file_name>*

For Example:

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

SRV Addresses

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

E2. 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 Dr.Web 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 Dr.Web 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 in operation of the updating system:

- for peer Dr.Web Servers, use identical configuration,
- for subordinate Dr.Web 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 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
```

.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
```

.proto

The .proto file contains the name of the protocol which is used to receive updates from the updates servers.

May take one of the following values: http | https | ftp | ftps | sftp | scp | smb | smbs | file.

> ⚠ The smb and smbs protocols are available only for Dr.Web Servers under UNIX system-based OS.

For Example:

```
https
```

.auth

The .auth file contains parameters of user authorisation 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
`cdn`	`on | off`	Using Content Delivery Network during repository loading: • `on`—use CDN, • `off`—do not use CDN.
`cert`	`drweb | valid | any | custom`	Allowed SSL certificates of update servers that will be automatically accepted: • `drweb`—accept only SSL certificate of Doctor Web company, • `valid`—accept only valid SSL certificates, • `any`—accept any certificates, • `custom`—accept certificate defined by user.
`cert-path`		Path to the user-defined if the `custom` mode of the `cert` parameter is set.
`ssh-mode`	`pwd | pubkey`	Authorization mode when using `scp` and `sftp` protocols (based on *ssh2*): • `pwd`—authorization by user login and password, • `pubkey`—authorization by encryption keys.
`ssh-pubkey`		Path to the public ssh key of update server.
`ssh-prikey`		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 Dr.Web 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 Dr.Web 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 Dr.Web 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 Dr.Web Server.

For Example:

- German, Chinese 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/cn-.*\.dwl$

^common/es-.*\.dwl$

^win/de-.*

^win/cn-.*

^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	• ON—freeze of product updates is enabled. • OFF—freeze of product updates is disabled.
UseFilter	YES|NO	• Yes—freeze updates only if updates files match the exceptions list in the .delay-only 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 Format

This section describes the format of the following files:

File	Description
drwcsd.conf	Dr.Web Server configuration file
webmin.conf	Dr.Web Security Control Center configuration file
download.conf	Configuration file to set up downloaded from the Dr.Web Server data
drwcsd-proxy.conf	Dr.Web Proxy Server configuration file
drwreploader.conf	Repository loader 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` Dr.Web Server configuration file resides by default in the `etc` subfolder of the Dr.Web Server installation folder. If Dr.Web 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 H3. Dr.Web Server).

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

1. Stop Dr.Web 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 Dr.Web Server configuration file.
4. Start Dr.Web Server (see **Administrator Manual**, p. Start and Stop Dr.Web Server).

Dr.Web Server Configuration File Format

Dr.Web Server configuration file is in XML format.

Description of Dr.Web Server configuration file parameters:

- `<version value="" />`

  Current version of the configuration file.

- `<name value="" />`

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

- `<id value="" />`

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

- `<passwd-salt value="" />`

  A cryptographic salt. A string of random data that is added to administrator password. The combined value is hashed by a hash function and stored as a single hash in the database to protect the password from brute force cracking. The salt is generated by default after installation or upgrade of Dr.Web Server from previous versions. An empty value prescribes not to use the password encryption (not recommended).

  > Viewing or changing the administrator password using the provided database management utility (`drwidbsh3`) is impossible when the salt is present.

  > When using a Dr.Web Server cluster, make sure to manually set the same salt value on every Dr.Web Server included in the cluster.

- `<location city="" country="" department="" floor="" latitude="" longitude="" organization="" province="" room="" street="" />`

  The Dr.Web Server geographic location.

  Attributes description:

Attribute	Description
`city`	City
`country`	Country
`department`	Department name
`floor`	Floor
`latitude`	Latitude
`longitude`	Longitude
`organization`	Organization name

Attribute	Description
`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 the Dr.Web 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** mode (`mode='open'`).	Empty value, which means assign the **Everyone** group as a primary.
`mode`	• 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.

- `<emplace-auto enabled="" />`

  Mode of creating station accounts in the Control Center when installing Agents via the group installation package, if accounts already created are not enough.

Attribute	Allowed values	Default
`enabled`	• `yes`—automatically create missing station accounts, • `no`—installation is possible only according to already created accounts in the group, installation package for stations of which is launched.	`yes`

- `<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 Dr.Web 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="" host="" />

  Replace NetBIOS names of computers with DNS names.

  Description of attributes:

Attribute	Allowed values	Description
enabled	• yes—replace, • no—do not replace. The <agent-host-names /> parameter will be used instead.	NetBIOS name replacement mode.
host	• yes—display partially qualified DNS names (before the dot in FQDN), • no—display fully qualified DNS names (FQDN).	Displayed name format after replacement.

- <agent-host-names mode="" />

  Displaying mode for computer names in anti-virus network when accessing Dr.Web Server. Allowed values of mode:

  - netbios—display NetBIOS names (used by default if the attribute is empty or the parameter is missing completely),
  - fqdn—display fully qualified DNS names (FQDN),
  - host—display partially qualified DNS names (before the dot in FQDN).

- <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`	• `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 the Dr.Web 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 Dr.Web 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 Dr.Web 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`	• `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 ans storing into the Dr.Web 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 station states ans storing the information into the Dr.Web 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 Dr.Web Server database. Allowed values of `enabled`: `yes` or `no`. Parameter is ignored for `<track-agent-status enabled="no" />`.

- `<track-agent-modules enabled="" />`

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

- `<keep-infection enabled="" />`

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

- `<keep-blocked-devices enabled="" />`

  Allow monitoring of information on devices blocked by the Office Control component and storing the information into the Dr.Web Server database. Allowed values of `enabled`: `yes` or `no`.

- `<keep-appcontrol-activity enabled="" />`

  Allow monitoring of processes activity at stations detected by Application Control (for filling Applications catalog) and storing the information into the Dr.Web Server database. Allowed values of `enabled`: `yes` or `no`.

- `<keep-appcontrol-block enabled="" />`

  Allow monitoring the blocking of the processes at stations by Application Control and storing the information into the Dr.Web 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 Dr.Web 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 Dr.Web Server to Agents.

  Attributes description:

Attribute	Allowed values	Description	Default
`queue-size`	• positive integer, • `unlimited`.	Maximum allowable number of updates distribution sessions running at the same time from Dr.Web Server. When the limit is reached, the Agent requests are placed into the waiting queue. The waiting queue size is unlimited.	`unlimited`
`value`	• 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`	• positive integer, • `unlimited`.	Maximum allowable number of the Agent installation sessions running at the same time from Dr.Web Server. When the limit is reached, the Agent requests are placed into the waiting queue. The waiting queue size is unlimited.	`unlimited`
`value`	• 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`	• `yes`—allow synchronization, • `no`—disable synchronization.	Synchronization mode.
`startup-sync`	Positive integer.	Number of stations without geographical coordinates, information on which is requested when

Attribute	Allowed values	Description
		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 Dr.Web 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 Dr.Web 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 Dr.Web Server database. Allowed values of `enabled`: `yes` or `no`.

- `<proxy auth-list="" enabled="" host="" password="" user="" />`

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

  Attributes description:

Attribute	Allowed values	Description
`auth-list`	• `none`—do not use authorization, • `any`—any supported method, • `safe`—any safe supported method, • the following methods, if several, set all necessary methods separated by a space: ▫ `basic` ▫ `digest` ▫ `digestie` ▫ `ntlmwb` ▫ `ntlm` ▫ `negotiate`	Proxy server authorization type. Default is 'any'.
`enabled`	• `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.

When setting the list of allowed authorization methods for a proxy server, you can use the `only` mark (add it to the end of the list with a space) to change the algorithm of authorization method selecting.

For more details, see https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html.

- `<statistics enabled="" id="" interval="" />`

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

  Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	• `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 Dr.Web Servers will be exchanging 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.

- `<multicast-updates enabled="" />`

  Allows to configure update transmission to workstations via multicast protocol. Allowed values of `enabled`: `yes` or `no`.

  `<multicast-updates>` contains multiple child elements and attributes:

Child element	Attribute	Description	Default
`port`	`value`	The Dr.Web Server's network interface port number that is used by transport multicast	2197

Child element	Attribute	Description	Default
`<port value="" />`		protocol to transmit the updates. This port is used by all multicast groups. For multicast updates, you must specify any unused port that will be different from the one specified in the Dr.Web Server's transport protocol settings.	

`ttl`
`<ttl value="" />`
	`value`	Time-to-live of transferred UDP-datagram. This value will be used by all multicast groups.	8

`group`
`<group address="" />`
	`address`	IP address of a multicast group the stations will receive multicast updates from.	233.192.86.0 for IPv4
			FF0E::176 for IPv6

`on`
`<on interface="" ttl="" />`
	`interface`	IP address of Dr.Web Server network interface that transport multicast protocol is bound to for updates transmission.	–

	`ttl`	Time-to-live of a UDP-datagram transferred through specified network interface. Has a higher priority than the general `<ttl value="" />` child element.	8

`transfer`
`<transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" announce-send-times="" />`
	`datagram-size`	UDP datagram size (bytes)—size of UDP datagrams in bytes.
		Allowed range is 512–8192. To avoid fragmentation, it is recommended that you set a value less than MTU (Maximum Transmission Unit) of the network.
			1400

	`assembly-timeout`	File transmission time (ms.)—during the specified time, single update file is transmitted, after that Dr.Web Server starts sending the next file. All files, which failed to transmit as a part of multicast protocol update, will be transmitted as a part of standard update process over the TCP protocol.	180000
	`updates-interval`	Duration of multicast updates (ms.)—duration of update process via multicast protocol.	600000

Child element	Attribute	Description	Default
		All files that failed to transmit at the stage of updating via multicast protocol will be transmitted as a part of the standard update via TCP protocol.	
	`chunks-interval`	Package transmission interval (ms.)—interval of package transmission to a multicast group. The low interval value may cause significant losses during package transfer and overload the network. It is not recommended to change this parameter.	14
	`resend-interval`	Interval between requests for retransmission (ms.)—at this interval Agents send out requests for retransmission of lost packages. Dr.Web Server accumulates these requests and sends out any lost blocks afterwards.	1000
	`silence-interval`	“Silence” interval on the line (ms.)—whenever a file transmission is over before the allowed time has expired and if during a specified “silence” interval no requests for retransmission of lost packages are received from Agents, Dr.Web Server assumes that all Agents successfully received update files and initiates transmission of the next file.	10000
	`accumulate-interval`	Retransmission request accumulation interval (ms.)—during the specified interval, Dr.Web Server accumulates requests from Agents for retransmission of lost packages. Agents request for lost packages. Dr.Web Server accumulates these requests throughout the specified time and sends out any lost blocks afterwards.	2000
	`announce-send-times`	Number of file transmission announcements—A number of times Dr.Web Server announces a file transmission to a multicast group before the update transmission starts. The announcement means a UDP-datagram with file metadata, which is sent to a	3

Child element	Attribute	Description	Default
		multicast group. Increasing the number of announcements can potentially improve transmission reliability, but at the same time can lead to decreased amount of data that can be transmitted over the multicast protocol for the time allowed.	

Optionally, `<multicast-updates>` can also contain the `<acl>` child element, which is used to create ACL lists. This allows restricting a scope of workstation TCP addresses that are authorized to receive multicast updates over multicast protocol from the current Dr.Web Server. `<acl>` is not present initially, which means no restrictions are applied by default.

`<acl>` includes the following child elements:

- `<priority mode="" />`

  Sets the list 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 are only the addresses included in the `<allow>` list and not included in the `<deny>` list.

- `<allow>`

  A list of TCP addresses, which are allowed to receive updates over the multicast protocol. 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 `address` attribute defines network addresses in the following format: *<IP address>*`/[`*<prefix>*`]`.

- `<deny>`

  The list of TCP addresses, which are not allowed to receive updates over the multicast protocol. 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 `address` attribute defines network addresses in the following format: *<IP address>*`/[`*<prefix>*`]`.

- `<database connections="" />`

  Database definition.

  Attributes description:

Attribute	Allowed values	Description	Default
`connections`	Positive integer.	Maximal number of connections of Dr.Web Server with database. It is recommended to change default value only after consultation with the technical support.	2

Attribute	Allowed values	Description	Default
`speedup`	`yes | no`	Automatically perform the delayed purging of the database after its initialization, upgrade and import (see **Administrator Manual**, p. Database).	`yes`

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="" cache="" cachesize="" readuncommitted="" precompiledcache="" synchronous="" openmutex="" checkintegrity="" autorepair="" mmapsize="" wal="" wal-max-pages="" wal-max-seconds="" />`

Defines SQLite3 embedded database.

Attributes description:

Attribute	Allowed values	Description	Default
`dbfile`		Database name.	`database.sqlite`
`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 bytes).	1048576
`synchronous`	• `TRUE` or `FULL`—synchronous • `FALSE` or `NORMAL`—regular • `OFF`—asynchronous	Data write mode.	`FULL`
`checkintegrity`	`quick | full | no`	Verify integrity of database image at Dr.Web Server startup.	`quick`
`autorepair`	`yes | no`	Automatically restore corrupted database image at Dr.Web Server startup.	`no`

Attribute	Allowed values	Description	Default
`mmapsize`	Positive integer.	Maximum number of bytes of the database file that is allowed to be mapped into the process address space at one time.	• for UNIX—10485760 • for Windows—0
`wal`	`yes | no`	Use Write-Ahead Logging.	`yes`
`wal-max-pages`		Maximal number of “dirty” pages on reaching of which pages will been written on the disk.	1000
`wal-max-seconds`		Maximal time to delay writing the pages on the disk (in seconds).	30

- `<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 file 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 https://www.postgresql.org/docs/9.1/libpq-connect.html	
`requiressl`	• `1 | 0` (via Control Center) • `y | n` • `yes | no` • `on | off`	Allow SSL connections only.	• `0` • `y` • `yes` • `on`
`user`		Database user name.	
`password`		Database user password.	
`temp_tablespaces`		Namespace for temporary tables.	

Attribute	Allowed values	Description	Default
`default_transaction_isolation`	• `read uncommitted` • `read committed` • `repeatable read` • `serializable`	Transaction isolation level.	`read committed`

- `<oracle connectionstring="" user="" password="" client="" prefetch-rows="0" prefetch-mem="0" />`

  Defines Oracle external database.

  Attributes description:

Attribute	Allowed values	Description	Default
`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 later 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.	
`prefetch-rows`	0-65535	Number of rows to be prefetched when executing a query to the database.	0—use the value = 1 (database default)
`prefetch-mem`	0-65535	Memory allocated for rows to be prefetched when executing a query to the database.	0—unlimited

- `<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`

Attribute	Allowed values	Description	Default
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	• SERIALIZABLE—serializable • READ_UNCOMMITTED—read uncommitted data • READ_COMMITTED—read committed data • REPEATABLE_READ—repeatable read • DEFAULT—equal ""—depends on DBMS.	Transaction isolation level. Some DBMS support READ_COMMITTED only.	DEFAULT

- `<mysql dbname="drwcs" host="localhost" port="3306" user="" password="" ssl="no" debug="no" />`

Defines MySQL/MariaDB external database.

Attributes description:

Attribute	Allowed values	Description	Default
dbname		Database name.	drwcs
host	Either of the two.	Database server address for TCP/IP connections.	localhost
		Path to UNIX socket file when using UDS. If not set, Dr.Web Server tries to locate the file in one of standard mysqld directories.	/var/run/mysqld/
port	Either of the two.	Port number to connect to the database via TCP/IP.	3306
		UNIX socket file name when using UDS.	mysqld.sock
user		Registration name of database user.	""
password		Database user password.	""

Attribute	Allowed values	Description	Default
`ssl`	`yes` | any other string	Allow SSL connections only.	`no`
`precompiledcache`	Positive integer.	Cache size of precompiled sql operators (in bytes).	1048576

- `<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 Dr.Web 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 Dr.Web Server.
  - `<agent>`—the list of limitations on IP addresses from which Dr.Web Agents can connect to this Dr.Web Server.
  - `<links>`—the list of limitations on IP addresses from which neighbor Dr.Web Servers can connect to this Dr.Web Server.
  - `<discovery>`—the list of limitations on IP addresses from which broadcast queries can be received by the *Dr.Web 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	• yes, • no.	Log information on the Dr.Web Server scripts execution profiling. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.	no
stack		Log information on Dr.Web 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.	
trace		Log information on Dr.Web 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, then 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 Dr.Web Server schedule.

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

  - `<hooks>`—paths for the user hooks of Dr.Web Server.

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

- `<transports>`

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

  Attributes description:

Attribute	Description	Obligatory	Allowed values	Default
discovery	Defines whether the Dr.Web Server detection service is used or not.	no, specified with the ip attribute only.	yes, no	no
• ip • unix	Defines the family of used protocols and specifies the interface address.	yes	–	• 0.0.0.0 • -
name	Specifies the Dr.Web Server name for the Dr.Web Server detection service.	no	–	drwcs
multicast	Defines whether Dr.Web Server included into a multicast group or not.	no, specified with the ip attribute only.	yes, no	no
multicast-group	Specifies the address of the multicast group into which Dr.Web Server is included.	no, specified with the ip attribute only.	–	• 231.0.0.1 • [ff18::231.0.0.1]
port	Port to listen.	no, specified with the ip 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	• yes—protocol is enabled, • no—protocol is disabled.	Protocol usage mode.	no
name	• AGENT—protocol that allows interaction of Dr.Web Server with Dr.Web Agents. • MSNAPSHV—protocol that allows interaction of Dr.Web Server with the Microsoft NAP Validator component of system health validating. • INSTALL—protocol that allows interaction of Dr.Web Server with Dr.Web Agent installers. • CLUSTER—protocol for interaction between Dr.Web Servers in the cluster system. • SERVER—protocol that allows interaction of 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	• yes—extension is enabled, • no—extension is disabled.	Extension usage mode.	no
name	• WEBMIN—Dr.Web Security Control Center extension for managing Dr.Web Server and anti-virus network via the Control Center. • FrontDoor—Dr.Web Server FrontDoor extension that allows connections of Dr.Web Server remote diagnostics utility.	Extension name.	-

- `<license>`

  Licensing settings.

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

  - `<limit-notify min-count="" min-percent="" />`

    Options for notification on limitation on a number of licenses in the license key.

    Attributes description:

Attribute	Description	Default
min-count	Maximal number of remaining licenses for which the **Limitation on a number of licenses in the license key** notification will be sent.	3
min-percent	Maximal percentage of remaining licenses for which the **Limitation on a number of licenses in the license key** notification will be sent.	5

  - `<license-report report-period="" active-stations-period="" />`

    Options for the report on license usage.

    Attributes description:

Attribute	Description	Default
report-period	Period of reports creation by Dr.Web Server on license keys it uses. If a report on license usage is created by a child Dr.Web Server, then after it is created, this report is sent to the main Dr.Web Server.	1440

Attribute	Description	Default
	Created reports are additionally sent at each connection (including restart) of Dr.Web Server, and also at changing the number of donated licenses at the main Dr.Web Server.	
`active-stations-period`	Period for counting the number of active stations for creating the report on licenses usage. The 0 value prescribes to count all stations in the report not depending on their activity status.	0

- `<exchange>`

  Settings of licenses propagation between Dr.Web Servers.

  The `<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 Dr.Web Server. The setting is used if the Server donates licenses to neighbor Dr.Web Servers.	1440
`prolong-preact`	**Period for accepted licenses renewal**—period till the license expiration, starting from which this Dr.Web Server initiates renewal of the license which is accepted from the neighbor Dr.Web Server. The setting is used if Dr.Web Server accepts licenses from neighbor Dr.Web Servers.	60
`check-interval`	**License synchronization period**—interval for synchronising information about donating licenses between Dr.Web 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`

Attribute	Allowed values	Description	Default
debug	• 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	• yes—use this authentication type, • no—do not use this authentication type.	Encrypt data transfer. At this, switching to secured connection is performed by using the STARTTLS command. The 25 port is used by default for the connection.	yes
auth_plain		Use *plain text* authentication on a mail server.	no
auth_login		Use *LOGIN* authentication on a mail server.	no
auth_cram_md5		Use *CRAM-MD5* authentication on a mail server.	no
auth_digest_md5		Use *DIGEST-MD5* authentication on a mail server.	no
auth_ntlm		Use *AUTH-NTLM* 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	• yes—use SSL, • no—do not use SSL.	SSL encryption usage mode.	no
verify_cert	• yes—check SSL sertificate, • no—do not check SSL sertificate.	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="" aggregation-period="" check-period="" threshold="" most-active="" />`

Configuration of parameters for tracking virus epidemic in the network.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	yes | no	Enables monitoring of multiple events of infecting stations and be able to send summary notifications to the administrator.	yes
aggregation-period	Positive integer.	Time period in seconds after sending the notification about epidemic, during which single notifications about infected stations will not be sent.	300
check-period		Time period in seconds, during which specified number of messages on infected stations must be received, to send the corresponding notification about epidemic.	3600
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 (the **Epidemic in the network** notification).	100

Attribute	Allowed values	Description	Default
`most-active`		Number of the most frequently occurring threats which must be included in the epidemic report.	5

- `<track-hips-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configuration of parameters for tracking multiple events of Preventive protection component.

  Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes | no`	Enables monitoring of multiple events of Preventive protection and be able to send summary notifications to the administrator.	`yes`
`aggregation-period`	Positive integer.	Time period in seconds after sending a summary report on Preventive protection events, during which notifications about single events will not be sent.	300
`check-period`		Time period in seconds, during which specified number of Preventive protection events must be occurred to send a summary report.	3600
`threshold`		The number of the Preventive protection events that must be received in specified time period, so that Dr.Web Server may send to the administrator a single summary report on these events (the **Summary report of Preventive protection** notification).	100
`most-active`		Number of the most frequently occurring processes that have performed a suspicious action, which must be included in the Preventive protection report.	5

- `<track-appctl-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configuration of parameters for tracking multiple events of Application Control component.

  Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes | no`	Enables monitoring of multiple events of Application Control and be able to send summary notifications to the administrator.	`yes`
`aggregation-period`	Positive integer.	Time period in seconds after sending a summary report on processes blocked by Application	300

Attribute	Allowed values	Description	Default
		Control, during which notifications about single blockings will not be sent.	
`check-period`		Time period in seconds, during which specified number of processes must be blocked to send a summary report.	3600
`threshold`		The number of events on processes blocked by Application Control that must be received in specified time period, so that Dr.Web Server may send to the administrator a single summary report on these events (the **Large number of blocks by the Application Control detected** notification).	100
`most-active`		Number of the most common profiles according to which the block was made, and which must be included in the notification on multiple blockings.	5

- `<track-disconnect enabled="" aggregation-period="" check-period="" single-alert-threshold="" summary-alert-threshold="" min-session-duration="" />`

  Configuration of parameters for tracking multiple abnormally terminated connections with clients.

  Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes | no`	Enables monitoring of abnormally terminated connections with clients and be able to send corresponding notifications to the administrator.	`yes`
`aggregation-period`	Positive integer.	Time period in seconds after sending the notification on multiple connections termination, during which notifications about single terminated connections will not be sent.	300
`check-period`		Time period in seconds, during which specified number of connections with clients must be terminated, to send the corresponding notification.	3600
`single-alert-threshold`		Minimum number of connections with a single address that must be terminated during the counting period, to send the notification about single abnormally terminated connection (the **Connection terminated abnormally** notification).	10

Attribute	Allowed values	Description	Default
`summary-alert-threshold`		Minimum number of connections that must be terminated during the counting period, to send the common notification about multiple abnormally terminated connections (the **Large number of abnormally terminated connections detected** notification).	1000
`min-session-duration`		If duration of terminated connection with a client is less than specified value, then specified number of connections is reached, notification about single terminated connections (the **Connection terminated abnormally** notification) will be sent not depending on the counting period. At this, the connection must not be terminated further by the longer connections, and the notification about multiple abnormally terminated connections must not be sent (the **Large number of abnormally terminated connections detected** notification).	300

- `<default-lang value="" />`

  Default language which is used by components and systems of Dr.Web Servers if failed to get language settings from the Dr.Web Server database. Particularly used by Dr.Web Security Control Center and administrator notification system if the database has been corrupted and the language settings cannot be obtained.

G2. Dr.Web Security Control Center Configuration File

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

  Parameter is specified in the following format:

  <Dr.Web Server IP address or DNS name>`[:`*<port>*`]`

  If the Dr.Web Server address is not specified, computer name returned by the operating system or the Dr.Web 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 Dr.Web 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 Dr.Web 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 the Dr.Web 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.X.

  Attributes description:

Attribute	Description	Default
`timeout`	HTTP session timeout. For persistent connections, Dr.Web 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

Attribute	Description	Default
`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
`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.

- `<xheaders>`

  Configuration parameter that lets you add custom HTTP headers. Three headers present by default are intended to protect from network attacks:

  - `<xheader name="X-XSS-Protection" value="1; mode=block"/>`

    The header controls web browser behavior if it detects any code inlined into attacked web page (so called "XSS attack"). Allowed values:

Value	Browser behavior
`0`	XSS filtering is disabled.
`1`	XSS filtering is enabled. Web browser will delete inline code if it detects an XSS attack.
`1; mode=block`	XSS filtering is enabled. Web browser will not render a compromised web page if it detects an XSS attack. This value is used by default.
`1; report=<network-address>`	XSS filtering is enabled. Web browser will delete inline code and report to specified address if it detects an XSS attack. This value is supported in Chromium-based web browsers only.

  - `<xheader name="X-Content-Type-Options" value="nosniff"/>`

    The header with the default value (`nosniff`) prevents web browser from executing any files implying MIME type changing.

- `<xheader name="X-Frame-Options" value="SAMEORIGIN"/>`

  The header controls web browser behavior if it detects an attempt to inline a web page into a frame (so called "clickjacking"). Allowed values:

Value	Browser behavior
DENY	Prevents web browser from rendering a web page in a frame.
SAMEORIGIN	Allows web browser to render a web page in a frame as long as the page and the frame both have the same origin (domain, port, and protocol). This value is used by default.
ALLOW-FROM <network-address>	Allows web browser to render a web page in a frame only if the web page is located at a specified address.

- `<reverse-resolve enabled=""/>`

  Replace IP address with DNS names of computers in the Dr.Web Server log file. Allowed values of enabled: `yes` or `no`.

- `<script-errors-to-browser enabled=""/>`

  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="" stack=""/>`

  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	• yes—enable profiling, • no—disable profiling.	Scripts profiling mode.
stack	• yes—log data, • no—do not log data.	Logging mode of information on profiling (function parameters and returned values) into the Dr.Web 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`
`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.	• `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 Dr.Web 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 Dr.Web Server and the port, which are used to connect the Agent Installer to Dr.Web Server, in the following format:

```
download = { server = '<Dr.Web_Server_Address>'; port = <port_number> }
```

where:

- *<Dr.Web_Server_Address>*—IP address or DNS name of Dr.Web Server.

  During generating of the Agent installation file, Dr.Web Server address is taken from the `download.conf` file first. If the Dr.Web 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 Dr.Web 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** → the **Network** tab → the **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 Dr.Web Server.

G4. Dr.Web Proxy Server Configuration File

The drwcsd-proxy.conf configuration file of the Proxy Server is presented in the XML format and located in the following folder:

- Windows OS: C:\ProgramData\Doctor Web\drwcs\etc
- Linux OS: /var/opt/drwcs/etc
- FreeBSD OS: /var/drwcs/etc

Description of Dr.Web Server configuration file parameters:

- <listen spec="">

  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 element attributes:

Attribute	Obligatory	Allowed values	Description	Default
ip | unix	yes	—	Type of the protocol for receiving incoming connections. Address which the Proxy Server listens is set as an attribute.	0.0.0.0 | -
port	no	—	Port which the Proxy Server listens.	2193
discovery	no	yes, no	The mode of the Dr.Web Server imitation. Allows detection of the Proxy Server as Dr.Web Server by the Network scanner.	yes
multicast	no	yes, no	Network "listening" mode for receiving multicast requests by the Proxy Server.	yes
multicast-group	no	—	Multicast group where the Proxy Server is located.	231.0.0.1 [ff18::231.0.0.1]

  Depending on the protocol, the list of non-obligatory properties in the spec attribute may vary.

  The list of non-obligatory properties, which can be set (+) or cannot be set (-) in the spec attribute, depending on the protocol:

Protocol	Attribute presence			
	port	discovery	multicast	multicast-group
`ip`	+	+	+	+
`unix`	+	–	–	–

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

The forwarding algorithm for the list of Dr.Web Servers is given in the **Administrator Manual**.

- `<compression mode="" level="">`

The `<compression />` element is a child of the `<listen />` element, it defines compression parameters for the client—Proxy Server channel.

Attributes description:

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

- `<encryption mode="">`

The `<encryption />` element is a child of the `<listen />` element, it defines encryption parameters for the client—Proxy Server channel.

Attributes description:

Attribute	Allowed values	Description	Default
`mode`	`yes`	Encryption enabled.	`possible`
	`no`	Encryption disabled.	
	`possible`	Encryption possible.	

- `<forward to="" master="">`

Specifies the settings to redirect the incoming connections. The `<forward />` element is obligatory. Several `<forward />` elements can be set with the different attribute values.

Attributes description:

Attribute	Allowed values	Description	Obligatory
`to`	An address is specified according to the The Specification of Network Addresses, particularly, in the following format: `tcp/`*<DNS_name>*`:`*<port>*.	Addresses of Dr.Web Server where to redirect the connection.	yes
`master`	• `yes`—Dr.Web Server is unconditional managing. • `no`—Dr.Web Server is not managing under any conditions. • `possible`—Dr.Web Server will be managing only if there are no explicit managing Dr.Web Servers (with the `yes` value for the `master` attribute).	The attribute defines if the Proxy Server settings can be remotely edited via the Control Center of Dr.Web Server specified in the `to` attribute. You can assign managing to any number of Dr.Web Servers (set the `master="yes"`); Proxy Server connects to all the managing Dr.Web Servers by their order in the settings until it gets the first valid (not empty) configuration. Also, you can assign none of the Dr.Web Servers managing (set the `master="no"`). In this case, the Proxy Server parameters (including the assignment of managing Dr.Web Servers) can be configured only locally via the Proxy Server configuration file.	no

If the `master` attribute is absent for Dr.Web Server, default is the same as `master="possible"`.

In the configuration file created by the installer during the Proxy Server installation, the `master` attribute is not defined for any of Dr.Web Servers.

- `<compression mode="" level="">`

If the `<compression />` element is a child of the `<forward />` element, it defines compression parameters for Dr.Web Server—Proxy Server channel. Attributes are the same as described above.

- `<encryption mode="">`

If the `<encryption />` element is a child of the `<forward />` element, it defines encryption parameters for Dr.Web Server—Proxy Server channel. Attributes are the same as described above.

- `<update-bandwidth value="" queue-size="">`

The `<update-bandwidth />` element allows to specify the speed limitation on updates transferring from Dr.Web Server to clients and the number of clients that downloading updates at the same time.

Attributes description:

Attribute	Allowed values	Description	Default
`value`	• KB/sec. • `unlimited`	Maximum summary speed of updates transferring.	`unlimited`
`queue-size`	• positive integer • `unlimited`	Maximum allowable number of updates distribution sessions running at the same time from Dr.Web Server. When the limit is reached, the Agent requests are placed into the waiting queue. The waiting queue size is unlimited.	`unlimited`

  - `<bandwidth value="" time-map="" />`

  The `<update-bandwidth />` element may have one or several `<bandwidth />` child elements. This element allows to specify speed limitation of data transferring for the specified time period.

  Attributes description:

Attribute	Allowed values	Description	Default
`value`	• KB/sec. • `unlimited`	Maximum summary speed of data transferring for the Agent updates.	`unlimited`
`time-map`	—	The mask that specifies the time period to apply limitations.	—

> The `time-map` attribute value is set automatically once the corresponding setting is configured in the Control Center web interface (see **Administrator manual**, p. Remote Configuration of the Proxy Server). As of today, there is no convenient way to set `time-map` manually from the configuration file.

- `<install-bandwidth value="" queue-size="">`

The `<install-bandwidth>` element allows to specify the speed limitation on data transferring during Agents installation and number of clients that downloading data for installation at the same time.

Attributes description:

Attribute	Allowed values	Description	Default
`value`	• KB/sec. • `unlimited`	Maximum summary speed of data transferring during the Agents installation.	`unlimited`

Attribute	Allowed values	Description	Default
queue-size	• positive integer • unlimited	Maximum allowable number of the Agent installation sessions running at the same time from Dr.Web Server. When the limit is reached, the Agent requests are placed into the waiting queue. The waiting queue size is unlimited.	unlimited

- `<bandwidth value="" time-map="">`

The `<install-bandwidth>` element may have one or several `<bandwidth />` child elements. This element allows to specify speed limitation of data transferring for the specified time period.

Attributes description:

Attribute	Allowed values	Description	Default
value	• KB/sec. • unlimited	Maximum summary speed of data transferring for the Agent installation.	unlimited
time-map	—	The mask that specifies the time period to apply limitations.	—

The time-map attribute value is set automatically once the corresponding setting is configured in the Control Center web interface (see **Administrator manual**, p. Remote Configuration of the Proxy Server). As of today, there is no convenient way to set time-map manually from the configuration file.

- `<cache enabled="">`

Configure the settings of Proxy Server repository cache.

Attributes description:

Attribute	Allowed values	Description	Default
enabled	yes | no	Defines if the caching is enabled.	yes

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

Element	Allowed values	Description	Default
`<clean-interval value="">`	positive integer	Number of stored revisions.	3
`<unload-interval value="">`	positive integer	Time slot between purging of old revisions in minutes.	60
`<repo-check mode="">`	positive integer	Time slot between unloads of unused files from the memory in minutes.	10

Element	Allowed values	Description	Default
`<repo-check />`	`idle	sync`	Check of cache integrity either at start (may take time) or in background.	`idle`

- `<synchronize enabled="" schedule="">`

Settings for synchronization of Proxy Server and Dr.Web Server repositories.

Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes	no`	Defines if the repository synchronization is enabled.	`yes`
`schedule`	—	Schedule for synchronization of the specified products.	—

The `schedule` attribute value is set automatically once the corresponding setting is configured in the Control Center web interface (see **Administrator manual**, p. Remote Configuration of the Proxy Server). As of today, there is no convenient way to set `schedule` manually from the configuration file.

The `<product name="" />` child elements give the list of products for the synchronization:

- 05-drwmeta—Dr.Web Server security data,
- 10-drwbases—virus databases,
- 10-drwgatedb—SpIDer Gate bases,
- 10-drwspamdb—Anti-spam bases,
- 10-drwupgrade—Dr.Web Updater,
- 15-drwhashdb—known hashes of threats,
- 20-drwagent—Dr.Web Agent for Windows,
- 20-drwandroid11—Dr.Web for Android databases,
- 20-drwcs—Dr.Web Server,
- 20-drwunix—Dr.Web Agent for UNIX,
- 20-drwcsdoc—documentation,
- 40-drwproxy—Dr.Web Proxy Server,
- 70-drwextra—Dr.Web enterprise products,
- 70-drwutils—Dr.Web administrative utilities,
- 80-drwnews—Doctor Web News.

- `<events enabled="" schedule="">`

Settings for caching the events received from the Agents.

Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes | no`	Defines if the caching is enabled. If enabled, the events are sent to Dr.Web Server according to the timetable. If the caching is disabled, events will be sent to Dr.Web Server immediately after receiving by the Proxy Server.	`yes`
`schedule`	—	Timetable according to which the events from the Agents will be transmitted.	—

> The `schedule` attribute value is set automatically once the corresponding setting is configured in the Control Center web interface (see **Administrator manual**, p. Remote Configuration of the Proxy Server). As of today, there is no convenient way to set `schedule` manually from the configuration file.

- `<update enabled="" schedule="">`

  Settings for the automatic update of the Proxy Server.

  For the automatic update, if the synchronization is enabled, the Proxy Server updates are downloaded from Dr.Web Server according to the synchronization timetable (see above) and are installed according to the update timetable (by default, with no time limitations). If the synchronization is disabled, when updates are downloaded and installed by update timetable (by default, with no time limitations).

  Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes | no`	Defines if the automatic update is enabled.	`yes`
`schedule`	—	Timetable according to which the updates will be downloaded (if synchronization is not set) and installed.	—

> The `schedule` attribute value is set automatically once the corresponding setting is configured in the Control Center web interface (see **Administrator manual**, p. Remote Configuration of the Proxy Server). As of today, there is no convenient way to set `schedule` manually from the configuration file.
>
> By default, the automatic update is allowed with no time limitations.

- `<core-dump enabled="" maximum="">`

  The 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: `%APPDATA%\Doctor Web\drwcsd-proxy\dump\`

Attributes description:

Attribute	Allowed values	Description	Default
`enabled`	`yes | no`	Defines if dumps collecting is enabled.	`yes`
`maximum`	positive integer	Maximal dumps number. The oldest are deleted.	10

- `<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`	• `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.

G5. Repository Loader Configuration File

The `drwreploader.conf` Repository Loader configuration file is presented in the XML format and located in the etc subfolder of the Dr.Web Server installation folder.

To use the configuration file

- For the console utility, the path to the file must be specified in the `--config` switch.
- For the graphical utility, the file must reside in the utility folder. If the utility is ran without configuration file, it will be created in the utility folder and will be used at next launches.

Description of the Repository Loader configuration file parameters:

- `<mode value="" path="" archive="" key="">`

  Attributes description:

Attribute	Description	Allowed values
`value`	Updates loading mode: • `repository`—repository is downloaded in the Dr.Web Server repository format. Loaded files can be directly imported via the Control Center as the Dr.Web Server repository updates. • `mirror`—repository is downloaded in the GUS updates zone format. Loaded files can be placed on the updates mirror in your local network. Further, Dr.Web Servers can be configures to receive updates directly from this updates mirror containing the last version of the repository but not from the GUS servers.	`repository | mirror`
`path`	The folder for downloading the repository.	–
`archive`	Pack downloaded repository into a zip archive automatically. This option allows to get prepared archive file for import downloaded repository archive to Dr.Web Server via the Control Center, for the **Administrating → Repository Content** section.	`yes | no`
`key`	Dr.Web license key file. Instead of a license key you can specify only MD5 hash of a license key, which you can view in the Control Center in the **Administration → License Manager** section.	–

- `<log path="" verbosity="" rotate="">`

  Repository Loader log settings.

  Attributes description:

Attribute	Description	Allowed values
`path`	Path to the log file.	–
`verbosity`	Log level of detail. `TRACE3` is by default.	`ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT`. The `ALL` and `DEBUG3` values are synonyms.
`rotate`	Repository Loader log rotation mode in the format: *<N><f>,<M><u>*. Same as the Dr.Web Server log rotation. By default, it is `10,10m`, which means storing of 10 files 10 megabytes each, use compression.	–

- `<update url="" proto="" cdn="" update-key="" version="">`

  General repository loading settings.

  Attributes description:

Attribute	Description	Allowed values
`url`	A GUS servers folder where updates of Dr.Web products are located.	–
`proto`	The protocol type to receive updates from update servers. For all protocols, updates are downloaded according to the settings of the GUS servers list.	`http | https | ftp | ftps | sftp | scp | file`
`cdn`	Allow downloading repository from GUS via Content Delivery Network	`yes | no`
`update-key`	Path to a public key or to a folder with a public key to validate the signature of updates that are loaded from GUS. The `update-key-*.upub` public keys to validate updates can be found on Dr.Web Server in the `etc` folder.	–
`version`	The Dr.Web Server version to which the updates must be loaded.	–

- `<servers>`

Update servers list. GUS servers are listed in the order the utility contacts them when downloading the repository.

Contains the `<server>` child elements with update servers.

- `<auth user="" password="">`

User credentials to authenticate on updates server, if the updates server requires authorization.

Attributes description:

Attribute	Description
user	User name at updates server.
password	Password at updates server.

- `<proxy host="" port="" user="" password="" />`

Parameters for connecting to the GUS via the proxy server.

Attributes description:

Attribute	Description
host	The network address of the proxy server.
port	The port number of the proxy server. Default is 3128.
user	User name on the proxy server if used proxy server requests authorization.
password	Password on the proxy server if used proxy server requests authorization.

- `<ssl cert-mode="" cert-file="">`

The type of SSL certificates that will be automatically accepted. This option is used only for secure protocols that support encrypting.

Attributes description:

Attribute	Description	Allowed values
cert-mode	Certificated to accept automatically.	any—accept all certificates, valid—accept only valid certificates, drweb—accept only Dr.Web certificates. custom—accept user-defined certificates.
cert-file	Path to the cert file.	–

- `<ssh mode="" pubkey="" prikey="">`

The type of the authorization on the update server when accessing by SCP/SFTP.

Attributes description:

Attribute	Description	Allowed values
mode	Authorization type.	▫ pwd—authorization using a password. A password is set in the <auth /> tag. ▫ pubkey—authorization using a public key. A public key is set in the pubkey attribute or extracted from the private key specified in the prikey.
pubkey	Public SSH key	–
prikey	Private SSH key	–

- <products>

  Loading products settings.

  - <product name="" update="">

  Each product settings separately.

  Attributes description:

Attribute	Description	Allowed values
name	Product name.	• 05-drwmeta—Dr.Web Server security data, • 10-drwbases—virus databases, • 10-drwgatedb—SpIDer Gate bases, • 10-drwspamdb—Anti-spam bases, • 10-drwupgrade—Dr.Web Updater, • 15-drwhashdb—known hashes of threats, • 20-drwagent—Dr.Web Agent for Windows, • 20-drwandroid11—Dr.Web for Android databases, • 20-drwcs—Dr.Web Server, • 20-drwunix—Dr.Web Agent for UNIX, • 20-drwcsdoc—documentation, • 40-drwproxy—Dr.Web Proxy Server, • 70-drwextra—Dr.Web enterprise products, • 70-drwutils—Dr.Web administrative utilities, • 80-drwnews—Doctor Web News.
update	Enable this product downloading.	yes | no

- <schedule>

  The schedule to receive updates periodically. At this, you do not have to launch the utility manually, the repository downloading performed automatically according to the specified time slots.

- `<job period="" enabled="" min="" hour="" day="" />`

Settings of scheduled loading execution.

Attribute	Description	Allowed values
`period`	Periodicity for loading task execution.	• `every_n_min`—every N minutes, • `hourly`—every hour, • `daily`—every day, • `weekly`—every week.
`enabled`	Downloading task is enabled.	`yes | no`
`min`	Minute to execute the task.	integers from 0 to 59
`hour`	Hour to execute the task. Relevant for `daily` and `weekly`.	integers from 0 to 23
`day`	Day to execute the task. Relevant for `weekly`.	• `mon`—Monday, • `tue`—Tuesday, • `wed`—Wednesday, • `thu`—Thursday, • `fri`—Friday, • `sat`—Saturday, • `sun`—Sunday.

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

Command line parameters have a higher priority than the default settings, or other constant settings (set in the Dr.Web 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 Appendix H, are 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.

In order to force run a command as administrator on operating systems of Windows family, you can use the `elevate` parameter. In this case, it shall be placed before all other switches and parameters, for instance: `drwcsd elevate start`.

H1. 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-certificate.pem"
```

Allowed switches

- `/compression` <*mode*>—compression mode of the traffic with Dr.Web 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 Dr.Web Server side.

  If the switch is not set, the `possible` value is used by default.
- `/encryption` <*mode*>—encryption mode of the traffic with Dr.Web 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 Dr.Web 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 Dr.Web Server. If authorization parameters are not set, authorization decision is defined on the Dr.Web 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 <*certificate*>—full path to the Dr.Web Server certificate.

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

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

- `/pwd` <*password*>—the Agent password to access Dr.Web Server.

  The switch is specifying with the `/id` switch for automatic authorization on Dr.Web Server. If authorization parameters are not set, authorization decision is defined on the Dr.Web 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 Dr.Web Server by sending multicast requests. If Dr.Web Server has not responded after the specified attempts number is reached, it is assumed that Dr.Web Server is not found.

  If the switch is not set, 3 attempts to find Dr.Web Server are performed.

- `/server [`<*protocol*>`/]`<*server_address*>`[:`<*port*>`]`—the Dr.Web 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 Dr.Web 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 Dr.Web 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.

H2. Dr.Web Agent for Windows

The start instruction format

```
es-service.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 Dr.Web Server. I.e. even if permissions to change the Agent settings are denied on Dr.Web Server, you can change these settings via the command line switches.

Allowed switches

- Show help:
  - `-?`
  - `--help`
- Change address of Dr.Web Server to which the Agent connects:
  - `-e` *<Dr.Web_Server>*
  - `--esserver=`*<Dr.Web_Server>*

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

  ```
  es-service -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
  ```

  or

  ```
  es-service --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 (the `%ProgramFiles%\DrWeb` folder by default), 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` and no longer used.

All public keys which were used previously (keys transmitted from Dr.Web Server and stored in the registry) are remained and used.

- Add the Dr.Web Server certificate:
  - `-c` *<certificate>*
  - `--addcert=`*<certificate>*

  Dr.Web Server certificate file specified as an argument is copied to the Agent folder (the `%ProgramFiles%\DrWeb` folder by default), is renamed to `drwcsd-certificate.pem` (if the name differs) and reread by the service. At this, previous certificate file, if presented, is renamed to `drwcsd-certificate.pem.old` and no longer used.

  All certificates which were used previously (certificates transmitted from Dr.Web Server and stored in the registry) are remained and used.

- Reconnect to the Server as a newbie:
  - `-w` *<value>*
  - `--newbie=`*<value>*

  Valid values: `once, always`. When set to `always` , the authorization parameters of the Agent are reset every time the service is started, and the Agent always connects to the Server as a newbie (see **Administrator Manual**, the New Stations Approval Policy section for more details). When set to `once` , the authorization parameters of the Agent will be reset the next time the service is started, after which the Agent will reconnect to the Server as a newbie just once.

- Change the Agent log details level:
  - `--change-loglevel=`*<level>*

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

  This switch works only under administrator rights and does not require switching off Self-Protection or manually restart of the service or OS.

H3. Dr.Web Server

There are several variants as how to launch Dr.Web Server. These variants will be described separately.

Several commands require `modexec` or `modexecdb` switches specified in command line to execute Lua modules and submit auxiliary parameters, if necessary. Such a command shall be written in the following way:

```
drwcsd [<switches>] modexec [<function_name>@]<module_name> [<parameters>]
```

- *<function_name>* — name of a specific function to be executed from a Lua module.
- *<module_name>* — name of a Lua module to be executed.

Commands described in p. H3.1. Managing Dr.Web Server—H3.5. Backup of Dr.Web Server Critical Data are cross-platform and enable using in both Windows OS and UNIX system-based OS, unless it is specified otherwise.

If an error occurred while launching Dr.Web Server management commands, please refer to the Dr.Web Server log file to find possible causes (see **Administrator Manual**, p. Dr.Web Server Log).

H3.1. Managing Dr.Web Server

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

H3.2. Basic Commands

- `drwcsd restart`—restart Dr.Web Server (it is executed as the `stop` and then `start` pair).
- `drwcsd start`—run Dr.Web Server.
- `drwcsd stop`—stop Dr.Web Server.
- `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).
- `drwcsd modexec agent@verify-key` *<full_key_filename>*—verify the license key file (`agent.key`).
- `drwcsd modexec enterprise@verify-key` *<full_key_filename>*— verify the Dr.Web Server license key file (`enterprise.key`). Please note that the Dr.Web Server license key file is no longer used from the version 10.
- `drwcsd verifyconfig` *<full_config_filename>*—verify the syntax of the Dr.Web Server configuration file (`drwcsd.conf`).
- `drwcsd verifycache`—verify content of the Dr.Web Server's file cache.
- `drwcsd syncads`—synchronize the network structure: Active Directory containers that contain computers become anti-virus network groups where workstations are placed into.

H3.3. Database Commands

Database Initialization

For initialization, the database must be absent or empty.

`drwcsd [`*<switches>*`] modexecdb database-init [`*<license_key>*` [`*<password>*`]]`— database initialization.

- *<license_key>*—path to Dr.Web license key file `agent.key`. If the license key is not specified, it must be added later from the Control Center or get from the neighbor Dr.Web Server via the interserver connection.

- *<password>*—original password of the Dr.Web Server administrator (logged in as **admin**). The default password is **root**.

> If you need to skip one or several parameters when writing the command, use the special value `%nil` instead of each skipped parameter.
>
> `%nil` can be omitted, if the next parameters are not set.

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 modexecdb database-init@<response-file>
```

<response-file>—file with initialization parameters written line-by-line in the same order same as parameters of the `database-init` command.

File format:

```
<full_license_key_filename>

<administrator_password>
```

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

If a string consists of only the `%nil` value, the default value is used (as in `database-init`).

Database Upgrading

`drwcsd modexecdb database-upgrade [pretend=false]`—run Dr.Web Server to upgrade the structure of the database to a new version using the internal scripts.

- `pretend=false` — instructs to check that the database schema is up-to-date instead of the actual upgrade of its structure. `false` by default. If `true`, it will only make sure that the database schema is up-to-date.

Database Export

a) `drwcsd modexecdb database-export` *<file>*—export the database to a 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
modexecdb database-export "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 modexecdb database-export-xml` <*xml_file*>—export the database to a 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 modexecdb database-export-xml 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 modexecdb database-export-xml database.gz
```

Example for UNIX system-based OS:

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

```
/etc/init.d/drwcsd modexecdb database-export-xml /test/database.db
```

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

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.gz
```

Database Import

a) `drwcsd modexecdb database-import` <*file*>—import the database from a specified file (the previous content of the database is deleted).

b) `drwcsd modexecdb database-import-and-upgrade` <*file*>—import and upgrade the database exported from Dr.Web Server of previous version (the previous content of the database is deleted).

⚠ Before using the `database-import-and-upgrade` command, you are strongly advised to back up the database.

Any problems during execution of these commands may lead to deletion of all information from the database.

You can use the `database-import-and-upgrade` command to import and upgrade the version of the database only within the same DBMS.

Database Verification

`drwcsd modexecdb database-verify [full=false [ignore-version=false]]`—run Dr.Web Server to verify the database. In order to record the results into a log file, the command shall be followed by a `-log` key. Details on how to use the key are described in H3.8. The Description of Switches.

- `full=false` — defines the verification type. By default (`false`) a quick check is made, if `true` —a full verification.
- `ignore-version=false` — defines whether the database schema version needs to be ignored during verification. `false` by default. If `true`, verification will continue even if the schema version is wrong.

Database Speed Up

`drwcsd [<`*switches*`>] modexecdb database-speedup`—execute the `VACUUM`, `CLUSTER`, `ANALYZE` commands to speed up the DB operation.

Database Restore

`drwcsd repairdb`—repair malformed disk image of **SQLite3** embedded database or corrupted tables of **MySQL** external database.

SQLite3 may be also automatically recovered on the Dr.Web Server startup if in the **SQLite3** database settings in the Control Center, the **Restore corrupted image automatically** flag is set (see **Administrator Manual**, p. Database Restore).

Database cleanup

`drwcsd modexecdb database-clean`—clean up the Dr.Web Server database by deleting all tables.

Administrator password reset

`drwcsd modexecdb set-admin-password` *<login> <new_password>*—set a new password for the specified administrator account.

H3.4. Repository Commands

> ⚠ You must necessarily stop Dr.Web Server before launching the `syncrepository`, `restorerepo` and `saverepo` commands.

- `drwcsd syncrepository`—synchronize the repository with Dr.Web GUS. The command launches the Dr.Web Server process, at this, GUS is called with the following repository update if updates are present.
- `drwcsd rerepository`—reread the repository from the drive. Under UNIX system base OS, similar to the `readrepo` command.
- `drwcsd updrepository`—update the repository from Dr.Web GUS. The command sends the signal to the operating Dr.Web Server process to call the GUS and perform the following repository update if updates are present. If Dr.Web Server is not running, the repository update is not performed.
- `drwcsd [`*<switches>*`] restorerepo` *<full_archive_name>*—restore repository of Dr.Web Server from the specified zip archive created via the `saverepo` command.
- `drwcsd [`*<switches>*`] saverepo` *<full_archive_name>*—save all repository of Dr.Web Server to the specified zip archive. Created archive can be imported to Dr.Web Server via the `restorerepo` command.

> ! Archives used by the `restorerepo` and `saverepo` commands are not compatible with archives used for repository export and import via the Control Center.

H3.5. Backup of Dr.Web Server Critical Data

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

```
drwcsd -home=<path> backup [<directory> [<quantity>]]
```

- Copy critical Dr.Web Server data to the specified *<directory>*.
- The `-home` switch sets the Dr.Web Server installation folder.
- *<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
```

All files in the backup except the database contents, are ready to use. The database backup copy is stored in the `.gz` format compatible with `gzip` and other archivers. The database contents can be imported from the backup copy to another database of Dr.Web Server, thus restore the data (see p. Restoring the Database of Dr.Web Enterprise Security Suite).

During the operation, Dr.Web Server regularly stores backup copies of important information into the following folders:

- for **Windows** OS: <*installation_drive*>`:\DrWeb Backup`
- for **Linux** OS: `/var/opt/drwcs/backup`
- for **FreeBSD** OS: `/var/drwcs/backup`

To perform the back up, a daily task is included into the Dr.Web Server schedule. If such task is missing in the schedule, it is recommended to create it.

H3.6. Commands for Windows OS Only

- `drwcsd [`<*switches*>`] install [`<*service_name*>`]`—install the Dr.Web Server service in the system and assign specified switches to launch this service.

  <*service_name*> is a suffix that is added to the default name of the service; at this, the full name of the service is `DrWebES-`<*service_name*>. The `install` command creates (edits) the service with specified name and automatically adds the `-service=`<*service_name*> switch into its arguments. At this, existing services remain unchanged.

- `drwcsd uninstall [`<*service_name*>`]`—uninstall the Dr.Web Server service from a system.

  <*service_name*> is a suffix that is added to the default name of the service; at this, the full name of the service is `DrWebES-`<*service_name*>.

- `drwcsd kill`—perform emergency shutdown of the Dr.Web Server service (if normal termination failed). This instruction should not be used without extreme necessity.
- `drwcsd reconfigure`—reread and reboot the configuration file (it is performed quicker and without starting a new process).
- `drwcsd silent [`<*options*>`]` <*command*>—disable messages from Dr.Web Server when launching the <*command*>. Used particularly in command files to disable the Dr.Web Server interactivity.

H3.7. Commands for UNIX System-Based OS Only

- `drwcsd cacherepo` — create or recreate the Dr.Web Server repository file cache.
- `drwcsd config`—similar to `reconfigure` or `kill SIGHUP` commands—restart Dr.Web Server.

- `drwcsd interactive`—run Dr.Web Server but do not direct the control to the process.
- `drwcsd newkey`—generate a new encryption keys `drwcsd.pri` and `drwcsd.pub` and the `drwcsd-certificate.pem` certificate.
- `drwcsd readrepo`—reread repository from the drive. Similar to the `rerepository` command.
- `drwcsd selfcert[`<*hostname*>`]`—generate a new SSL certificate (`certificate.pem`) and RSA private key (`private-key.pem`). The parameter specifies the host name with Dr.Web Server installed for which the files are generated. If the name is not specified, it will be gotten automatically by a system function.
- `drwcsd shell` <*file_name*>—run the script file. The command launches `$SHELL` or `/bin/sh` and passes the specified file.
- `drwcsd showpath`—show all program paths, registered in the system.
- `drwcsd status`—show the current status of Dr.Web Server (running, stopped).

H3.8. The Description of Switches

Cross-platform switches

- `-activation-key=`<*license_key*>—Dr.Web Server license key. By default, it is the `enterprise.key` file located in the etc subfolder of the root folder.

  Please note that the Dr.Web Server license key file is no longer used from the version 10. The –`activation-key` switch may be used during the Dr.Web Server upgrade from the previous versions and database initialization: the Dr.Web Server identifier will be taken from the specified license key.
- `-bin-root=`<*folder*>—the path to executable files. By default, it is the `bin` subfolder of the root folder.
- `-conf=`<*file*>—name and location of the Dr.Web 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 the Dr.Web 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 modexecdb database-verify` instruction, see above.
- `-help`—displays help. Similar to the programs described above.
- `-hooks`—to permit Dr.Web Server to perform user extension scripts located in the:
  - for Windows OS: `var\extensions`
  - for FreeBSD OS: `/var/drwcs/extensions`
  - for Linux OS: `/var/opt/drwcs/extensions`

subfolder of the Dr.Web Server installation folder. The scripts are meant for automation of the administrator work enabling quicker performance of certain tasks. All scripts are disabled by default.

- `-home=`<*folder*>—Dr.Web 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_file*>—activate logging to the file at the specified path.

  For Dr.Web Servers under UNIX system-based OS, the "minus" sign can be used instead of the filename, which instructs standard output of the log.

  By default: for Windows OS, it is `drwcsd.log` in the folder specified by the `-var-root` switch, for UNIX system-based OS, it is set by the `-syslog=user` switch (see below).
- `-private-key=`<*private_key*>—private encryption key of Dr.Web Server. By default, it is `drwcsd.pri` in the `etc` subfolder of the root folder.
- `-rotate=`<*N*><*f*>`,`<*M*><*u*>—Dr.Web Server log rotation mode, where:

Parameter	Description
<*N*>	Total number of log files (including current and archive).
<*f*>	Log files storing format, possible values: • 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: • to set rotation by log file size: ▫ k—Kb, ▫ m—Mb, ▫ g—Gb. • to set rotation by time: ▫ 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 `10z,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*>—path to a folder to which Dr.Web 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=`<*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.

  If necessary, it is possible to set specific levels of detail for several message sources at once in the following format:

  `-verbosity=`<*message_source1*>`:`<*level1*>`,`<*message_source2*>`:`<*level2*>`,` <*message_source3*>`:`<*level3*> and so on. In this case, <*level*> is inherited on general principle, i.e. it looks for the closest parental source with specified level of detail. The `-verbosity=all:all` switch is equal to the `-verbosity=all` switch (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.
- `-service=`<*service_name*>—the switch is used by running service process for self-identification and activation of the self-protection for the registry branch of the Dr.Web Server service. <*service_name*> is a suffix that is added to the default name of the service; at this, the full name of the service is `DrWebES-`<*service_name*>.

  The switch is used by the `install` command; independent use is not provided.

- `-screen-size=`<*size*>—(if run not as a service, but in the interactive mode)—log size in lines displayed in the Dr.Web Server screen, the default value is 1000.

Switches for UNIX system-based OS Only

- `-etc=`<*path*>—path to the `etc` (`<var>/etc`) directory.
- `-keep`—do not remove temporary directory after the Dr.Web Server installation.
- `-pid=`<*file*>—a file to which Dr.Web 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 Dr.Web Server with the `-syslog` key (e.g., `service drwcsd start -syslog=user`), the Dr.Web 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).

H3.9. 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 Linux OS: `/etc/init.d/drwcsd`.
- For FreeBSD OS: `/usr/local/etc/rc.d/drwcsd` (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
`-home`	DRWCS_HOME	• `/usr/local/drwcs`—for FreeBSD OS, • `/opt/drwcs`—for Linux OS.
`-var-root`	DRWCS_VAR	• `/var/drwcs`—for FreeBSD OS, • `/var/opt/drwcs`—for Linux OS.
`-etc`	DRWCS_ETC	`$DRWCS_VAR/etc`
`-rotate`	DRWCS_ROT	`10,10m`

Switch	Variable	Default parameters
`-verbosity`	DRWCS_LEV	`info`
`-log`	DRWCS_LOG	`$DRWCS_VAR/log/drwcsd.log`
`-conf`	DRWCS_CFG	`$DRWCS_ETC/drwcsd.conf`
`-pid`	DRWCS_PID	
`-user`	DRWCS_USER	
`-group`	DRWCS_GROUP	
`-hooks`	DRWCS_HOOKS	
`-trace`	DRWCS_TRACE	

`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		Additional command line instructions to deliver to `drwcsd` at start.
DRWCS_CORE	`unlimited`	The core file maximal size.
DRWCS_FILES	131170	The maximal number of file descriptors, that Dr.Web Server is able to open.
DRWCS_BIN	`$DRWCS_HOME/bin`	The directory to start the `drwcsd` from.
DRWCS_LIB	`$DRWCS_HOME/lib`	The directory with epy Dr.Web 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 /var/opt/drwcs/etc/common.conf file exists, it will be included in drwcsd, which could redefine some variables. However, if they are not exported (via the export command), they will not take any effect.

To set variables

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.

H3.10. Administration of Dr.Web Server Version for UNIX OS with the kill Instruction

The version of Dr.Web Server for UNIX OS is administrated by the signals sent to the Dr.Web 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 Dr.Web Server,
- SIGTERM—shut down Dr.Web Server,
- SIGQUIT—shut down Dr.Web Server,
- SIGINT—shut down Dr.Web Server.

Similar actions are performed by the switches of the drwcsd instruction for the Windows version of Dr.Web Server, read Appendix H3.3. Database Commands.

H4. 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 Dr.Web Server automatically and without fail.

H5. Dr.Web Proxy Server

To configure the Proxy Server parameters, run with corresponding switches the `drwcsd-proxy` executable file, which resides in the `bin` subdirectory of the Proxy Server installation directory.

The Start Instruction Format

`drwcsd-proxy [<switches>] [<commands> [<command_arguments>]]`

Allowed Switches

Cross-platform Switches

- `--console=yes|no`—run the Proxy Server in the interactive mode. At this, the Proxy Server operation log is written to the console.

  Default: `no`.

- `--etc-root=<path>`—path to the configuration files directory (`drwcsd-proxy.conf`, `drwcsd.proxy.auth` and etc.).

  Default: `$var/etc`

- `--home=<path>`—path to the Proxy Server installation directory.

  Default: `$exe-dir/`

- `--log-root=<path>`—path to the directory with the Proxy Server operation log files.

  Default: `$var/log`

- `--pool-size=<N>`—pool size for clients connections.

  Default: core number of the computer with the Proxy Server installed (not less than 2).

- `--rotate=<N><f>,<M><u>`—Proxy Server log rotation mode, where:

Parameter	Description
<N>	Total number of log files (including current and archive).
<f>	Log files storing format, possible values: • 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: • to set rotation by log file size: ▫ k—Kb, ▫ m—Mb,

Parameter	Description
	▫ g—Gb. • to set rotation by time: ▫ 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.

Default is `10,10m`, which means storing of 10 files of 10 megabytes each, use compression.

- `--trace=yes|no`—enable detailed logging of Proxy Server calls. Available only if the Proxy Server supports calls stack tracing (if an exception occurs, stack is written to the log).

  Default: `no`.

- `--tmp-root=`*<path>*—path to the temporary files directory. Is used at Proxy Server automatic update.

  Default: `$var/tmp`.

- `--var-root=`*<path>*—path to the Proxy Server working directory to store cache and database.

  Default:

  - Windows OS: `%ALLUSERSPROFILE%\Doctor Web\drwcs`
  - Linux OS: `/var/opt/drwcs`
  - FreeBSD OS: `/var/drwcs`

- `--verbosity=`*<details_level>*—log details level. Default is `TRACE`. Allowed values are: `ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT`. The `ALL` and `DEBUG3` values are synonyms.

  If necessary, it is possible to set specific levels of detail for several message sources at once in the following format:

  `-verbosity=`*<message_source1>*`:`*<level1>*`,`*<message_source2>*`:`*<level2>*`,` *<message_source3>*`:`*<level3>* and so on. In this case, *<level>* is inherited on general principle, i.e. it looks for the closest parental source with specified level of detail. The `-verbosity=all:all` switch is equal to the `-verbosity=all` switch (see also Appendix K. Log Files Format).

All switches for setting Proxy Server parameters can be set simultaneously.

Switches for UNIX system-based OS

- `--user`—set the user identifier. The switch is relevant for both, normal and daemon modes.
- `--group`—set the group identifier. The switch is relevant for both, normal and daemon modes.
- `--pid=`*<path>*—path to the directory with the process identifier.

  Default:`/var/opt/drwcs/run/drwcsd-proxy.pid`

Allowed Commands and their Arguments

If the command is not specified, the `run` command is used.

- `import` *<path>* `[`*<revision>*`]` `[`*<products>*`]`—import files from Dr.Web Server repository to the Proxy Server cache.
  - *<path>*—path to the directory with Dr.Web Server repository. The Dr.Web Server repository must be preliminary downloaded to the computer with the Proxy Server installed.
  - *<revision>*—maximum number of revisions to import. If the value is not set, all revision will be imported.
  - *<products>*—the list of products divided by the space that are intended to import. By default, the list is empty, i.e. import all repository products except Dr.Web Server. If the list is set, only the products from the list will be imported.
- `help`—show help message on switches for Proxy Server configuration.
- `run`—start the Proxy Server in normal mode.

For Windows OS only

- `install`—install the service.
- `start`—start the installed service.
- `stop`—stop the started service.
- `uninstall`—uninstall the service.

Commands available under UNIX system-based OS only:

- `daemon`—run the Proxy Server as a daemon (see also Switches for UNIX system-based OS).

Proxy server control script and variables available under UNIX system-based OS

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

- **Linux**: `/etc/init.d/dwcp_proxy`
- **FreeBSD**: `/usr/local/etc/rc.d/dwcp_proxy`

The script accepts the following commands:

- `import` *<path>* `[`*<revision>*`]` `[`*<products>*`]`—import files from Dr.Web Server repository to the Proxy Server cache (same as the command of Proxy Server—see above).
- `interactive`—run the Proxy Server in the interactive mode. At this, the Proxy Server operation log is written to the console.
- `start`—run the Proxy Server as a daemon.
- `status` — check if the daemon is launched.
- `stop`—stop the started daemon.

Correspondence between variables and command switches for the `drwcsd-proxy` is described in the Table H-3.

Table H-3.

Switch	Variable	Default parameters
`--home=`*<path>*	`$DRWCS_PROXY_HOME`	`$exe-dir/`
`--var-root=`*<path>*	`$DRWCS_PROXY_VAR`	• Linux OS: `/var/opt/drwcs` • FreeBSD OS: `/var/drwcs`
`--etc-root=`*<path>*	`$DRWCS_PROXY_ETC`	`$var/etc`
`--tmp-root=`*<path>*	`$DRWCS_PROXY_TMP`	`$var/tmp`
`--log-root=`*<path>*	`$DRWCS_PROXY_LOG`	`$var/log`
–	`$DRWCS_PROXY_LIB`	`$DRWCS_PROXY_HOME/lib`
–	`$DRWCS_PROXY_BIN`	`$DRWCS_PROXY_HOME/bin`
`--verbosity=`*<details_level>*	`$DRWCS_PROXY_VERBOSITY`	`INFO`
`--rotate=`*<N><f>*,*<M><u>*	`$DRWCS_PROXY_ROTATE`	`10,10m`
`--pid`	`$DRWCS_PROXY_PID`	`/var/opt/drwcs/run/drwcsd-proxy.pid`
-	`$NO_DRWCS_PROXY_USER`	If any value is assigned, the `$DRWCS_PROXY_USER` is ignored.
`-user`	`$DRWCS_PROXY_USER`	–

Switch	Variable	Default parameters
–	`$NO_DRWCS_PROXY_GROUP`	If any value is assigned, the `$DRWCS_PROXY_GROUP` is ignored.
`--group`	`$DRWCS_PROXY_GROUP`	–
–	`$DRWCS_PROXY_FILES`	131170 but not less than the current limit.

H6. 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.

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 `makeself` 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 contents of embedded LSM entry with basic information about the package: title, version, description, author, etc. A corresponding message will be displayed if the LSM entry is not filled in.
- `--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 delete the target folder once the embedded script is executed.
- `--nox11`—do not spawn the `xterm` terminal emulator once the installation is complete.
- `--nochown`—do not assign the user who initiated the installation as the owner of extracted files.
- `--log` <*path*>—enable installation logging into a file at a specified path.

- `--nolog`—do not log the installation.
- `--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.

Additional arguments

- `--help`—show the help on additional arguments.
- `--quiet`—run the installer in the background mode. The affirmative answer is used for all the following questions of the installer:
    - accept the license agreement,
    - set back up into the default folder,
    - continue the installation provided that extra distribution kit installed in the system will be deleted.
- `--clean`—install the package with the Dr.Web Server default settings not using the backup to restore the settings from the previous installation.
- `--preseed` *<path>*—path to the configuration file with predefined answers on installer questions during the installation.

  Variables to specify the predefined answers in the configuration file:
    - `DEFAULT_BACKUP_DIR=`*<path>*—path to the backup that is used for restoring the settings from the previous version (is not used if you set the installation not applying restore from the backup).
    - `QUIET_INSTALL=[0|1]`—defines the usage of the installer background mode:
        - 0—run the installer in the background mode;
        - 1—run the installer in the regular mode.
    - `CLEAN_INSTALL=[0|1]`—defines the usage of backup during the installation:
        - 0—install not applying backup;
        - 1—install applying restore from the backup located in the folder from the `DEFAULT_BACKUP_DIR` variable. If the `DEFAULT_BACKUP_DIR` variable is not specified, backup is taken from the `/var/tmp/drwcs`.
    - `ADMIN_PASSWORD=`*<password>*—password for default administrator account (**admin**).
        - If the `ADMIN_PASSWORD` variable is specified in the file, its value is used as the administrator password and the following message is displayed at the end of the installation:
          `Password specified in the configuration file for the default administrator (admin):` *<password>*
        - If the `ADMIN_PASSWORD` variable is not specified in the file, the password is generated automatically and the following message is displayed at the end of the installation:
          `Automatically generated password for the default administrator (admin):` *<password>*

If you use the `--preseed` argument and do not define the installer background mode in the configuration file via the `QUIET_INSTALL=0` variable, when the values of other variables of the configuration file will be redefined by a user during the installation.

H7. Utilities

H7.1. Digital Keys and Certificates Generation Utility

The following console versions of the digital keys and certificates generation utility are provided:

Executable file	Location	Description
`drweb-sign-<`*OS*`>-<`*bitness*`>`	Control Center, the **Administration → Utilities** section	Independent version of the utility. Can be launched from any directory or on any computer with corresponding operating system.
	The `webmin/utilities` Dr.Web Server directory	
`drwsign`	The `bin` Dr.Web Server directory	Utility version depends on server libraries. Can be launched only from its location directory.

> The `drweb-sign-<`*OS*`>-<`*bitness*`>` and `drwsign` utility versions are similar in their functions. Further in the section, the `drwsign` version is used, but all examples are relevant for both versions.

The start instruction format

- `drwsign check [-public-key=<`*public_key*`>] <`*file*`>`

  Check the specified file signature using a public key of the person who signed this file.

Switch parameter	Default value
<*public_key*>	`drwcsd.pub`

- `drwsign extract [-private-key=<`*private_key*`>] [-cert=<`*Dr.Web_Server_certificate*`>] <`*public_key*`>`

  Extract the public key from the private key file or from the certificate and write the public key to the specified file.

  The `-private-key` and `-cert` switches are mutually exclusive, i.e. only one switch can be set; if both switches are set at the same time, the command fails to execute.

  The switch parameters must be specified.

  If none of the switches is set, `-private-key=drwcsd.pri` is used to extract the public key of the `drwcsd.pri` private key.

Switch parameter	Default value
<*private_key*>	`drwcsd.pri`

- `drwsign genkey [`*<private_key>*` [`*<public_key>*`]]`

  Generate a public—private pair of keys and write them to the corresponding files.

Switch parameter	Default value
<private_key>	`drwcsd.pri`
<public_key>	`drwcsd.pub`

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

- `drwsign gencert [-private-key=`*<private_key>*`] [-subj=`*<subject_fields>*`] [-days=`*<validity_period>*`] [`*<self_signed_certificate>*`]`

  Generate a self-signed certificate using the Dr.Web Server private key and write it to the corresponding file.

Switch parameter	Default value
<private_key>	`drwcsd.pri`
<subject_fields>	`/CN=`*<hostname>*
<validity_period>	`3560`
<self_signed_certificate>	`drwcsd-certificate.pem`

- `drwsign gencsr [-private-key=`*<private_key>*`] [-subj=`*<subject_fields>*`] [`*<certificate_sign_request>*`]`

  Generate a request for the certificate signature based on the private key and write this request to the corresponding file.

  Can be used to sign the certificate of another server, e.g. to sign a Dr.Web Proxy Server certificate with the Dr.Web Server key.

  To sign such requests, use the `signcsr` switch.

Switch parameter	Default value
<private_key>	`drwcsd.pri`
<subject_fields>	`/CN=`*<hostname>*
<certificate_sign_request>	`drwcsd-certificate-sign-request.pem`

- `drwsign genselfsign [-show] [-subj=`*<subject_fields>*`] [-days=`*<validity_period>*`] [`*<private_key>*` [`*<self_signed_certificate>*`]]`

Generate a self-signed RSA certificate and an RSA private key for a web server and write them to the corresponding files.

The `-show` switch prints certificate content in a readable view.

Switch parameter	Default value
<subject_fields>	`/CN=`*<hostname>*
<validity_period>	`3560`
<private_key>	`private-key.pem`
<self_signed_certificate>	`certificate.pem`

- `drwsign hash-check [-public-key=`*<public_key>*`]` *<hash_file>* *<signature_file>*

  Check the signature of the specified 256-bit number in the client-server protocol format.

  In the *<hash_file>* parameter, the file with the 256-bit number to sign is specified. The *<signature_file>* file is the signature result (two 256-bit numbers).

Switch parameter	Default value
<public_key>	`drwcsd.pub`

- `drwsign hash-sign [-private-key=`*<private_key>*`]` *<hash_file>* *<signature_file>*

  Sign the specified 256-bit number in the client-server protocol format.

  In the *<hash_file>* parameter, the file with the 256-bit number to sign is specified. The *<signature_file>* file is the signature result (two 256-bit numbers).

Switch parameter	Default value
<private_key>	`drwcsd.pri`

- `drwsign help [`*<command>*`]`

  Print brief information on the program or on the specific command in the command line format.

- `drwsign sign [-private-key=`*<private_key>*`]` *<file>*

  Sign *<file>* using the private key.

Switch parameter	Default value
<private_key>	`drwcsd.pri`

- `drwsign signcert [-ca-key=`*<private_key>*`] [-ca-cert=`*<Dr.Web_Server_certificate>*`] [-cert=`*<certificate_to_sign>*`] [-days=`*<validity_period>*`] [-eku=`*<purpose>*`] [`*<signed_certificate>*`]`

  Sign the existing *<certificate_to_sign>* using the private key and the certificate of Dr.Web Server. The signed certificate is saved into a separate file.

Can be used to sign the Dr.Web Proxy Server certificate with the Dr.Web Server key.

The following values of the `-eku` switch (Extended Key Usage extension) can be used:

- `drwebServerAuth`—authentication of the Server/Proxy server by the Agent,
- `drwebMeshDAuth`—authentication of the Scanning server by the Virtual agent.

Switch parameter	Default value
<private_key>	`drwcsd.pri`
<Dr.Web_Server_certificate>	`drwcsd-ca-cerificate.pem`
<certificate_to_sign>	`drwcsd-certificate.pem`
<validity_period>	`3560`
<purpose>	`drwebServerAuth`
<signed_certificate>	`drwcsd-signed-certificate.pem`

- `drwsign signcsr [-ca-key=`*<private_key>*`] [-ca-cert=`*<Dr.Web_Server_certificate>*`] [-csr=`*<certificate_sign_request>*`] [-days=`*<validity_period>*`] [-eku=`*<purpose>*`] [`*<signed_certificate>*`]`

Sign *<certificate_sign_request>* generated by the `gencsr` command using the private key and the Dr.Web Server certificate. The signed certificate is saved into a separate file.

Can be used to sign the certificate of another server, e.g. to sign a Dr.Web Proxy Server certificate with the Dr.Web Server key.

The following values of the `-eku` switch (Extended Key Usage extension) can be used:

- `drwebServerAuth`—authentication of the Server/Proxy server by the Agent,
- `drwebMeshDAuth`—authentication of the Scanning server by the Virtual agent.

Switch parameter	Default value
<private_key>	`drwcsd.pri`
<Dr.Web_Server_certificate>	`drwcsd-cerificate.pem`
<certificate_sign_request>	`drwcsd-certificate-sign-request.pem`
<validity_period>	`3560`
<purpose>	`drwebServerAuth`
<signed_certificate>	`drwcsd-signed-certificate.pem`

- `drwsign tlsticketkey [`*<TLS_ticket>*`]`

Generate a TLS ticket.

Can be used in a Server cluster for shared TLS sessions.

Switch parameter	Default value
<TLS_ticket>	`tickets-key.bin`

- `drwsign verify [-ss-cert] [-CAfile=`*<Dr.Web_Server_certificate>*`]` `[`*<certificate_to_check>*`]`

  Check the validity of the certificate with the trusted certificate of the Server.

  The `-ss-cert` switch prescribes to ignore the trusted certificate and validate the self-signed certificate only.

Switch parameter	Default value
<Dr.Web_Server_certificate>	`drwcsd-certificate.pem`
<certificate_to_check>	`drwcsd-signed-certificate.pem`

- `drwsign x509dump [`*<certificate_to_print>*`]`

  Print the dump of any x509 certificate.

Switch parameter	Default value
<certificate_to_print>	`drwcsd-certificate.pem`

- `drwsign version`

  Show the utility version.

H7.2. Administrating Utility of the Embedded Database

For embedded database (SQLite3) management, you are provided with the `drwidbsh3` utility.

`drwidbsh3` resides in the following folders:

- on **Linux** OS: `/opt/drwcs/bin`
- on **FreeBSD** OS: `/usr/local/drwcs/bin`
- on **Windows** OS: *<Dr.Web_Server_installation_folder>*`\bin`

  (default Dr.Web Server installation folder is: `C:\Program Files\DrWeb Server`).

The start instruction format

`drwidbsh3` *<full_DB_filename>*

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

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

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

Example of drwidbsh3 usage to view or change administrator password:

> ⚠ This will work only if you disable administrator password encryption in the Dr.Web Server configuration file first. See details about the `passwd-salt` parameter in the section G1. Dr.Web Server Configuration File.

1. Run the `drwidbsh3` utility and specify path to the DB file:
   - For the embedded DB on Linux OS:

   ```
   /opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
   ```

   - For the embedded DB on Windows OS:

   ```
   "C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb
   Server\var\database.sqlite"
   ```

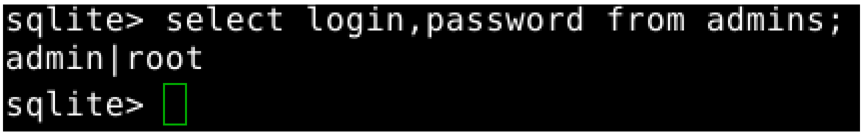
2. To view all data from the `admins` table, run the following command:

   ```
   select * from admins;
   ```

3. To view logins and passwords of all administrator accounts, run the following command:

   ```
   select login,password from admins;
   ```

4. As an example, 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 `drwidbsh3` utility, run the following command:

   ```
   .exit
   ```

H7.3. 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. Graphical version of the utility is available for Windows OS only.

You can download the utility via the Control Center, the **Administration** item in the main menu, the **Utilities** item in the control menu:

- For Windows OS—graphical version.
- For UNIX system-based OS—console version.

The following versions of Dr.Web Server remote diagnostics utility are provided:

Executable file	**Location**	**Description**
`drweb-cntl-`*<OS>*`-`*<bitness>*	Control Center, the **Administration** → **Utilities** section	Independent version of the utility. Can be launched from any directory or on any computer with corresponding operating system.
	The `webmin/utilities` Dr.Web Server directory	
`drwcntl`	The `bin` Dr.Web Server directory	Utility version depends on server libraries. Can be launched only from its location directory.

The `drweb-cntl-`*<OS>*`-`*<bitness>* and `drwcntl` version of the utility are similar in their functions. Further in the section, the `drwcntl` version is given, but all examples are relevant for both versions.

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

For connection of the utility (both graphical and console) using TLS, you must directly specify the protocol when setting the Dr.Web Server address: `ssl://`*<IP address or DNS name>*.

The Dr.Web 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 string of Dr.Web Server, to which the utility connects, in the following format: `[(tcp|ssl)://]`*<IP address or DNS name>*`[:`*<port>*`]`.

  To be able to connect via the one of the supported protocols, it is necessary to meet the following conditions:

  a) To connect via `ssl`, in the `frontdoor.conf` configuration file, the `<ssl />` tag must be set. At this, the connection can be established via `ssl` only.

  b) To connect via `tcp`, in the `frontdoor.conf` configuration file, the `<ssl />` tag must be disabled (commented). At this, the connection can be established via `tcp` only.

  If connection parameters are not set in the Dr.Web Server address string, the following values are used:

Parameter	Default value
Connection protocol	`tcp` ⚠ For the TCP connection, the **Use TLS** flag must be cleared in the Control Center, in the **Administration** → **Dr.Web Server remote access** section. This disables the `<ssl />` tag in the `frontdoor.conf` configuration file.
IP address or DNS name of Dr.Web Server	Utility prompts you to specify the Dr.Web Server address in the corresponding format.
Port	`10101` ⚠ At Dr.Web Server, allowed port is set in the **Dr.Web Server Remote Access** section and saved in the `frontdoor.conf` configuration file. If the alternative port is used in this section, it is necessary to set this port directly when connecting the utility.

- *<login>*—login of the Dr.Web Server administrator.
- *<password>*—administrative password to access Dr.Web Server.

  If administrative login and password are not set in the connection string, the utility prompts you to specify corresponding credentials.

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 Dr.Web 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.
    - `caddresses [`*<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 Dr.Web 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 Dr.Web 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 Dr.Web Server process dump.
- `cpu` <*parameter*>—show statistics of the computer CPU usage on which Dr.Web 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 Dr.Web Servers under UNIX system-based OS only.

- `die`—stop Dr.Web Server and write the Dr.Web Server process dump.

> The `die` command is available for Dr.Web Servers under UNIX system-based OS only.

- `dwcp` <*parameter*>—set/show Dr.Web Control Protocol (includes Dr.Web 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 Dr.Web 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,
  - `rawdw`—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 Dr.Web 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 Dr.Web 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 Dr.Web 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 Dr.Web Server is installed. To request the certain parameter, use the following commands:
    - `all`—shoe 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 Dr.Web 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 Dr.Web Servers under Windows OS, Linux system-based OS only,
> - `heap`—for Dr.Web Servers under Windows OS, Linux system-based OS only,
> - `malloc`—for Dr.Web Servers under Linux system-based OS and FreeBSD system-based OS only,
> - `sizes`—for Dr.Web 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 Dr.Web Server process. Allowed parameters:

    - `disable`—disable monitoring,
    - `enable`—enable monitoring,
    - `show`—show current mode.
- `printstat`—write the Dr.Web Server operation statistics 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 Dr.Web Server.
- `show` <*parameter*>—show the information about the system on which Dr.Web 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 Dr.Web Servers under Windows OS, Linux system-based OS only,
> - `mapping`—for Dr.Web Servers under Windows OS, Linux system-based OS only,
> - `limits`—for Dr.Web Servers under UNIX system-based OS only,
> - `processors`—for Dr.Web Servers under Linux system-based OS only.

- `sql`—execute SQL query.
- `stop`—stop Dr.Web Server.
- `traffic` <*parameter*>—show statistics on the Dr.Web Server network traffic. To request the certain parameter, use the following commands:
    - `all`—show all the traffic from the Dr.Web 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 Dr.Web 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 Dr.Web 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.

- `version` — show the utility version.

H7.4. Dr.Web Server Remote Scriptable Diagnostics Utility

Dr.Web Server remote diagnostics utility allows remotely connect to Dr.Web Server for basic controlling and viewing the operation statistics. Unlike the drwcntl, `the drwcmd` utility can be used at scripting.

The following console versions of Dr.Web Server remote scriptable diagnostics utility are provided:

Executable file	Location	Description
`drweb-cmd-<`*`OS`*`>-<`*`bitness`*`>`	Control Center, the **Administration → Utilities** section	Independent version of the utility. Can be launched from any directory or on any computer with corresponding operating system.
	The `webmin/utilities` Dr.Web Server directory	
`drwcmd`	The `bin` Dr.Web Server directory	Utility version depends on server libraries. Can be launched only from its location directory.

The drweb-cmd-<*OS*>-<*bitness*> and drwcmd version of the utility are similar in their functions. Further in the section, the drwcmd version is given, but all examples are relevant for both versions.

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

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

The start instruction format

drwcmd [<*switches*>] [<*files*>]

Allowed Switches

The drwcmd utility uses switches according the general rules described in the Appendix H. Command Line Parameters of the Programs Included in Dr.Web Enterprise Security Suite.

- --?—show help message on switches for using the utility.
- --help—show help message on switches for using the utility.
- --commands=<*commands*>—execute specified commands (similar to the drwcntl utility commands). To specify several commands, use the ; sign as a separator.
- --debug=yes|no—log utility operations in the debug mode (the stderr standard output stream). Default is no.
- --files=yes|no—allow execution of the commands (similar to the drwcntl utility commands) from the specified files. Default is yes.

  Commands must be set in a file by one on each line. Empty lines are ignored. Use the # sign to start a comment.
- --keep=yes|no—keep the connection with Dr.Web Server after the last command is executed till the completion of the utility process. Default is no.
- --output=<*file*>—output file for the Dr.Web Server response. By default, if the file is not specified, the stdout standard output stream is used.

If the file name starts with the (+), then the result of commands execution will be added to the end to file, otherwise—file will be rewritten.

- `--password=`<*password*>—password for the authorization at Dr.Web Server. Can be defined in the file set in the `--resource` switch.
- `--read=yes|no`—allow reading the Dr.Web Server connection parameters from the resource file. Default is `yes`.
- `--resource=`<*file*>—resource file with the Dr.Web Server connection parameters: the Dr.Web Server address and administrator credentials for the authorization at Dr.Web Server. By default, the `.drwcmdrc` file is used from the following directory:
    - For UNIX system-based OS: `$HOME`
    - For Windows OS: `%LOCALAPPDATA%`

  Each line in the file must contain 3 words separated by spaces: <*Dr.Web_Server*> <*user*> <*password*>.

  To specify the space in the middle of a word, use the `%S`. If you need the percent sign, use `%P`.

  For example:

```
ssl://127.0.0.1 user1 password1

ssl://127.0.0.1 user2 password2

ssl://127.0.0.1 user pass%Sword
```

> ⚠ When using the `--resource` switch, you must also specify the `--server` switch. Utility connects to Dr.Web Server specified in the `--server` switch according to the credentials that corresponds to the address of this Dr.Web Server from the resource file.

- `--server=`<*Server*>—the Dr.Web Server address. Default is `ssl://127.0.0.1`. Can be defined in the file set in the `--resource` switch.
- `--user=`<*user*>—user name for the authorization at Dr.Web Server. Can be defined in the file set in the `--resource` switch.
- `--verbose=yes|no`—print detailed response of Dr.Web Server (the `stdout` standard output stream). Default is `no`.
- `--version` — show the utility version.

The procedure for connecting to Dr.Web Server:

1. When defining the data for the Dr.Web Server connection, the priority are given to the values specified in the switches `--server`, `--user` and `--password`.
2. If the `--server` switch is not specified, the default value is used—`ssl://127.0.0.1`.
3. If the `--user` switch is not specified, then the necessary Dr.Web Server is searched in the `.drwcmdrc` file (can be redefined in the `--resource` switch) and first user name is taken in the alphabetical order.

4. If the `--password` switch is not specified, then the search is performed in the `.drwcmdrc` file (can be redefined in the `--resource` switch) by Dr.Web Server and user name.

   > User name and password will be read from the `.drwcmdrc` file (can be redefined in the `--resource` switch), if it is not forbidden by the `--read` switch.

5. If a user name and a password are not specified via the switches or the resource file, the utility prompts for credentials to be entered via the console.

Commands execution features:

- If the (–) values is set for the files with commands, then the utility reads command entered via the console.
- If both command in the `--commands` switch and the files list are set, then the commands from the `--commands` switch are executed first.
- If neither files of commands in the `--commands` switch are specified, then the commands entered via the console are read.

For example:

To execute the command from the `--command` switch and then a console commands, enter the following:

```
drwcmd --commands=<commands> -- -
```

Completion Codes

- 0—successful execution.
- 1—the help in switches is requested: `--help` or `--?`.
- 2—command line parse error: authorization parameters are not specified, etc.
- 3—cannot create output file for the Dr.Web Server response.
- 4—Dr.Web Server authorization error: wrong administrator's login and/or password.
- 5—Dr.Web Server connection terminated abnormally.
- 127—unknown fatal error.

H7.5. Dr.Web Repository Loader

> Graphical version of the Repository Loader utility is described in the **Administrator Manual** document, in the p. GUI Utility.

The following versions of Dr.Web Repository Loader console utility are provided:

Executable file	Location	Description
`drweb-reploader-<OS>-<bitness>`	Control Center, the **Administration** → **Utilities** section The `webmin/utilities` Dr.Web Server directory	Independent version of the utility. Can be launched from any directory or on any computer with corresponding operating system.
`drwreploader`	The `bin` Dr.Web Server directory	Utility version depends on server libraries. Can be launched only from its location directory.

The `drweb-reploader-<OS>-<bitness>` and `drwreploader` version of the utility are similar in their functions. Further in the section, the `drwreploader` version is given, but all examples are relevant for both versions.

To simplify specifying the switches to run the console utility, you can use the Repository Loader configuration file. In the pre-installed configuration file, the switches values correspond to the default values listed below, except the `--ssh-auth` switch: its value is redefined to the `pubkey` in the configuration file.

Possible Switches

- `--archive`—archive the repository. Default is `no`.
- `--auth` *<argument>*—credentials for authorization on the update server in the following format: *<user>*`[:`*<password>*`]`.
- `--cert-file` *<path>*—path to the root certificates storage for SSL authorization.
- `--cert-mode [`*<argument>*`]`—the type of SSL certificates that will be automatically accepted. This option is used only for secure protocols that support encrypting.

  The *<argument>* may take one of the following values:

  - `any`—accept all certificates,
  - `valid`—accept only valid certificates,
  - `drweb`—accept only Dr.Web certificates,
  - `custom`—accept user-defined certificates.

  The `drweb` value is used by default.
- `--config` *<path>*—path to the Repository Loader configuration file.
- `--cwd` *<path>*—path to the current working directory.
- `--ipc`—enable the transfer of data on the utility operation to the standard output stream. Default is `no`.

- `--help`—show help message on switches.
- `--license-key` *<path>*—path to the license key file (the key file or its MD5 hash must be specified).
- `--log` *<path>*—path to the log file on the repository downloading process.
- `--mode` *<mode>*—updates loading mode:
  - `repo`—repository is downloaded in the Dr.Web Server repository format. Loaded files can be directly imported via the Control Center as the Dr.Web Server repository updates. Value is used by default.
  - `mirror`—repository is downloaded in the GUS updates zone format. Loaded files can be placed on the updates mirror in your local network. Further, Dr.Web Servers can be configured to receive updates directly from this updates mirror containing the last version of the repository but not from the GUS servers.
- `--only-bases`—download only virus databases. Default is `no`.
- `--path` *<argument>*—download the repository from GUS to the folder specified as *<argument>*. When you archive the repository using the `--archive` switch, you can specify the path either to the folder name or to the archive file name. If the archive name is not specified, the `repository.zip` default name is used.
- `--product` *<argument>*—updated product. By default, entire repository is downloaded.
- `--prohibit-cdn`—deny CDN usage when downloading updates. Default is `no`, i.e. CDN is allowed to be used.
- `--proto` *<protocol>*—updates loading protocol: `file | ftp | ftps | http | https | scp | sftp | smb | smbs`. Default is `https`.
- `--proxy-auth` *<argument>*—data for authentication on the proxy server: user login and password in the following format: *<login>*`[:`*<password>*`]`.
- `--proxy-host` *<argument>*—proxy server address specified in the following format: *<server>*`[:`*<port>*`]`. Default is `3128`.
- `--rotate` *<N><f>*`,`*<M><u>*—Repository Loader log rotation mode. Same as the Dr.Web Server log rotation.

  By default, it is `10,10m`, which means storing of 10 files 10 megabytes each, use compression.
- `--servers` *<argument>*—GUS servers addresses. It is recommended to leave the default value: `esuite.geo.drweb.com`.
- `--show-products`—show the list of GUS products. Default is `no`.
- `--ssh-auth` *<type>*—type of the authorization on the update server when accessing by SCP/SFTP. For the *<type>* parameter, the one of the following values is allowed:
  - `pwd`—authorization using a password. A password is set in the `--auth` switch.
  - `pubkey`—authorization using a public key. You must specify a private key in the `--ssh-prikey` switch to extract corresponding public key.
- `--ssh-prikey` *<path>*—path to the SSH private key.
- `--ssh-pubkey` *<path>*—path to the SSH public key.

- `--strict`—terminate downloading if an error occurred. Default is `no`.
- `--update-key` *<path>*—path to a public key or to a folder with a public key to validate the signature of updates that are loaded from GUS. The `update-key-*.upub` public keys to validate updates can be found on Dr.Web Server in the `etc` folder.
- `--update-url` *<argument>*—GUS servers folder where updates of Dr.Web products are located. It is recommended to leave the default value: `/update`.
- `--V` — show the utility version.
- `--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.
- `--version` *<version>*—the Dr.Web Server version to download the updates for, in the following format: *<major_version>*`.`*<minor_version>*. For example, for Dr.Web Server of version 13, the *<version>* parameter is `13.00`. The availability of updates for specific products may differ depending on Dr.Web Server version. One way to confirm the available products is to check the `<products>` parameter description for Repository loader's configuration file in the manual for desired version.

Switches Usage Features

When launching the Repository Loader, please note the following rules:

Switches must be obligatory specified	**Condition**
`--license-key`	Always
`--update-key`	
`--path`	
`--cert-file`	If the following switches take one of the values: • `--cert-mode valid | drweb | custom`, • `--proto https | ftps | smbs`.
`--ssh-prikey`	If the following switches take one of the values: • `--proto sftp | scp`, • `--ssh-auth pubkey`.

Examples of Use

1. To create an imported archive with all products:

```
drwreploader.exe --path C:\Temp --archive --license-key C:\agent.key --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
```

```
Files\DrWeb Server\etc"
```

2. To create an imported archive with virus bases:

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" -only-bases
```

3. To create an imported archive with Dr.Web Server only:

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" --product=20-drwcs
```

H7.6. Dr.Web Agent for UNIX Remote Installation Utility

Dr.Web Agent for UNIX remote installation utility lets you install Dr.Web Agent on protected workstations running a UNIX system-based operating system in your anti-virus network. The utility can also be used to install Dr.Web for UNIX File Servers, if necessary.

The utility has a command-line interface and it is available in several versions:

Executable file	Location	Description
`drweb-unix-install-`*<OS>*`-`*<bitness>*	Control Center, the **Administration → Utilities** section	Independent version, which can be run from any directory and on any computer with a corresponding operating system. It is updated together with the repository or Dr.Web Server.
	The `webmin/utilities` Dr.Web Server directory	
`drwunixinstall`	The `bin Dr.Web` Server directory	A version, which depends on available server libraries and therefore, can be run from its original location only. It is updated together with the Dr.Web Server only.

The `drweb-unix-install-`*<OS>*`-`*<bitness>* and `drwunixinstall` versions are the same in terms of features. Further in this section, the `drwunixinstall` version is used, but the format and allowed switches are the same for both versions.

The start instruction format

`drwunixinstall [`*<switches>*`]`
<station_1_IP_address>`[:`*<SSH_port>*`[^`*<user_name>*`[^`*<password>*`]]]`
<station_2_IP_address>`[:`*<SSH_port>*`[^`*<user_name>*`[^`*<password>*`]]] ...`

Allowed Switches

The `drwunixinstall` utility uses switches according to the general rules described in Appendix H. Command Line Parameters of the Programs Included in Dr.Web Enterprise Security Suite.

- `--help` — show the help message.
- `--ak` *<authorization_parameters>* — set the alternative parameters of authorization on remote workstations using encryption keys in the following format:

```
<user_name>
^<path_to_Dr.Web_Server_private_key>
^<path_to_Dr.Web_Server_public_key>[^<private_key_password>]
```

If you set both the standard authorization parameters (the <*user_name*>^<*password*> pair) and the alternative parameters using encryption keys, the latter will be the used first when the utility is executed.

- `--ap` <*user_name*>^<*password*> — use the keyboard-interactive authorization on remote workstations.
- `--certificate` <*path*> — set a path to the Dr.Web Server certificate file. By default it is `webmin/install/unix/workstation/drwcsd-certificate.pem`.
- `--cpus` <*number*> — set a number of CPU cores to use for remote installation. By default it is `4`.
- `--ctimeout` <*time*> — set the maximum time to wait for installation package transferring to complete on remote workstations. Shall be specified in seconds, by default it is `600`.
- `--debug` — enable logging in debug mode. By default set to `no`.
- `--esuite` <*Dr.Web_Server_address*> — enter address of Dr.Web Server to be used for remote installation. The Agent will connect to this Dr.Web Server once the installation is complete. Shall be specified in the following format: `[udp://]`<*IP address or DNS name*>`[:`<*port*>`]`
- `--etimeout` <*time*> — set the maximum time to wait for package installation to complete on remote workstations. Shall be specified in seconds, by default it is `900`.
- `--from` <*path*> — set a path to a directory on Dr.Web Server containing the installation packages. By default it is `webmin/install/unix`.
- `--long` — enable logging with timestamps included. By default set to `no`.
- `--pwd` <*password*> — set a password for authorization on remote workstations while using the `su` and/or `sudo` command.
- `--remote-temp` <*path*> — set a path to a directory on remote workstations to temporarily store installation files and the Dr.Web Server's certificate. By default, the utility uses a temporary directory set in the operating system.
- `--server` — install Dr.Web for UNIX File Servers instead of Dr.Web Agent. By default set to `no`.
- `--simultaneously` <*number*> — set the maximum number of Dr.Web Agent installations on remote workstations at the same time.
- `--sshdebug` — enable logging in debug mode, with extra details on all operations using the SSH protocol. By default set to `no`.
- `--sshwaitdebug` — enable logging in debug mode, with extra detail on all operations using the SSH protocol and timer-related operations. By default set to `no`.
- `--stimeout` <*time*> — set the maximum time to wait for password input allowing the use of the `su` and/or `sudo` commands on remote workstations. Shall be specified in seconds, by default it is `10`.

- `--su` — use the `su` command during the installation to elevate privileges up to the root level on remote workstations. By default set to `no`.
- `--sudo` — use the `sudo` command during the installation to elevate privileges up to the root level on remote workstations. By default set to `no`.
- `--temp` <*path*> — set a path to a directory on Dr.Web Server to temporarily store the certificate. By default, the utility uses a temporary directory set in the operating system.
- `--timeout` <*time*> — set the maximum time to wait to establish connection and authenticate on remote workstations. Shall be specified in seconds, by default it is `30`.
- `--verbosity` <*details_level*> — set a level of detail while logging. By default it is `info`. Allowed values are `all, debug3, debug2, debug1, debug, trace3, trace2, trace1, trace, info, notice, warning, error, crit`. The `all` and `debug3` values are synonyms.
- `--version` — show the utility version.

H7.7. Dr.Web Agent for Windows Remote Installation Utility

Dr.Web Agent for Windows remote installation utility lets you install Dr.Web Agent on protected workstations running Windows in your anti-virus network.

The utility has a command-line interface and it is available in several versions:

Executable file	Location	Description
`drweb-windows-install-`<*OS*>`-`<*bitness*>	Control Center, the **Administration → Utilities** section	Independent version, which can be run from any directory and on any computer with a corresponding operating system. It is updated together with the repository or Dr.Web Server.
	The `webmin/utilities` Dr.Web Server directory	
`drwwindowsinstall`	The `bin Dr.Web` Server directory	A version, which depends on available server libraries and therefore, can be run from its original location only. It is updated together with the Dr.Web Server only.

The `drweb-windows-install-`<*OS*>`-`<*bitness*> and `drwwindowsinstall` versions are the same in terms of features. Further in this section, the `drwwindowsinstall` version is used, but the format and allowed switches are the same for both versions.

The start instruction format

`drwwindowsinstall` <*switches*>

Allowed Switches

> The `drwwindowsinstall` utility uses switches according to the general rules described in Appendix H. Command Line Parameters of the Programs Included in Dr.Web Enterprise Security Suite.

- `--help` — show the help message.
- `--console=yes|no` — print the utility logging to console. By default set to `no`.
- `--disable-v1=yes|no` — disable the SMB version 1 (SMBv1) protocol while the utility is working. By default set to `no`.
- `--distribution` *<file_name>* — manually enter the file name of the Agent installer, which will be run on remote workstations. By default it is `drwinst.exe`.
- `--install-address` *<workstation_IP_address>* — enter address of a remote station, where Dr.Web Agent will be installed to. If you specify several stations at once, make sure to divide their addresses with comma ("`,`") or semicolon ("`;`"), no spaces.
- `--install-certificate` *<path>* — set a path to the Dr.Web Server certificate file.
- `--install-clients` *<number>* — set the maximum number of the Agent installations on remote stations at a time. By default it is `8`.
- `--install-compression` *<mode>* — set the compression mode for traffic between Dr.Web Server and connected workstations: `on` to enable traffic compression, `off` to disable, `possible` to make it possible. The latter means that the mode depends on corresponding settings on Dr.Web Server. By default it is `possible`.
- `--install-encryption` *<mode>* — set the encryption mode for traffic between Dr.Web Server and connected workstations: `on` to enable traffic encryption, `off` to disable, `possible` to make it possible. The latter means that the mode depends on corresponding settings on Dr.Web Server. By default it is `possible`.
- `--install-language` *<language_code>* — set the installed Agent's interface language as a two-letter code according to the ISO 639-1 standard. If the switch is not used or Dr.Web Agent is not available in requested language, the remote station's default system language will be used instead.
- `--install-path` *<path>* — set a path to Dr.Web Agent installation directory on remote stations. By default it is `%ProgramFiles%\DrWeb`.
- `--install-register=yes|no` — register the Agent in the system list of installed software once the installation is complete. By default set to `no`.
- `--install-server` *<Dr.Web_Server_address>* — enter address of Dr.Web Server to be used for remote installation. The Agent will connect to this Dr.Web Server once the installation is complete. The switch format: `[udp://]`*<IP_address_or_DNS_name>*`[:`*<port>*`]`.
- `--install-timeout` *<time>* — set the maximum time to wait for the Agent installation to complete on remote workstations. Shall be specified in seconds, by default it is `300`.

- `--install-user` *<user_name>*`@`*<domain>*`:`*<password>* or *<domain>*`\`*<user_name>*`:`*<password>* — set user name and password to use for authorization on remote workstations.
- `--log` *<path>* — set a path to the utility log file. By default it is `drwsmb.log` in the `var` subdirectory of the Dr.Web Server installation directory.
- `--machine` *<name>* — specify the name to be assigned to a remote workstation in the Dr.Web Enterprise Security Suite anti-virus network once the Agent installation is compete and it is connected to Dr.Web Server. By default, a computer name registered in the operating system is used.
- `--rotate=`*<N><f>*`,`*<M><u>* — set the utility log rotation mode. The switch format is the same as the one used to manage the Dr.Web Server log rotation mode. By default it is `10,10m`.
- `--service-id` *<name_in_registry>* — set the registry key name to be assigned to the Agent remote installation service in the Windows registry. By default it is `DrWebRsvcRunner`.
- `--service-name` *<displayed_name>* — set the Agent remote installation service name as it is displayed in the Services snap-in. By default it is `Dr.Web Remote Runner Service`.
- `--target-root` *<directory_name>* — set the name of a directory in the administrative share on a remote station, which will be used to run the Agent installer copied from Dr.Web Server. By default it is `TEMP`.
- `--target-volume` *<share_name>* — set the administrative share name, which will contain the Agent installation files. By default it is `ADMIN$`.
- `--threads` *<number>* — set the number of I/O threads in a pool. By default set to `2`.
- `--verbosity` *<level>* — set the utility logging level. By default set to `trace`. Allowed values: `all, debug3, debug2, debug1, debug, trace3, trace2, trace1, trace, info, notice, warning, error, crit`. The `all` and `debug3` values are synonyms.
- `--version` — show the utility version.

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 Dr.Web Server catalogs is required. To this effect, Dr.Web 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 the Dr.Web Server launch; otherwise the current folder at launch.
- `DRWCSD_BIN`—path to the folder with executable files. The switch value is `-bin-root`, if it was set at the Dr.Web Server launch; otherwise it is the `bin` subfolder of the root folder.
- `DRWCSD_VAR`—path to the folder to which Dr.Web 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 the Dr.Web 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:

Symbol	Value
\	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:

Symbol	Value
\	general escape character
^	negate the class, but only if the first character
-	indicates character range

Symbol	Value
[	POSIX character class (only if followed by POSIX syntax)
]	terminates the character class

Appendix K. Log Files Format

Events on Dr.Web 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** (trace0..3—tracing)—enable tracing events according to the level of detail. (**Trace 3** instructs to log in the maximum level of detail);
  - **db0..3** (debug0..3—debugging)—instruct to log debugging events according to the 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 events** 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 automation 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. **Web API** accepts REST 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
asio	https://www.boost.org/LICENSE_1_0.txt*	https://think-async.com/Asio/
boost	https://www.boost.org/LICENSE_1_0.txt*	https://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.org/license.html*	https://c-ares.org/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html*	https://curl.se/libcurl/
ICU	https://www.unicode.org/copyright.html#License*	https://icu.unicode.org/home
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://www.freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	https://gcc.gnu.org/
HTMLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING*	https://github.com/jemalloc/jemalloc
jQuery	MIT License** GNU General Public License**	https://jquery.com/
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua

Third-party library	License	Project URL
Leaflet	BSD License https://github.com/Leaflet/Leaflet/blob/master/LICENSE*	https://leafletjs.com
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org
libssh2	3-Clause BSD License https://github.com/libssh2/libssh2/blob/master/COPYING*	https://www.libssh2.org/
libxml2	MIT License**	http://www.xmlsoft.org/
Linenoise NG	BSD license*	https://github.com/arangodb/linenoise-ng
lua	MIT License**	https://www.lua.org/
lua-xmlreader	MIT License**	https://asbradbury.org/projects/lua-xmlreader/
lzma	Public Domain	https://www.7-zip.org/sdk.html
ncurses	MIT License**	https://invisible-island.net/ncurses/announce.html
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
nghttp2	MIT License**	https://nghttp2.org/
Noto Sans CJK	https://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://fonts.google.com/noto/use
OpenLDAP	https://www.openldap.org/software/release/license.html*	https://www.openldap.org
OpenSSL	https://www.openssl.org/source/license.html*	https://www.openssl.org/

Third-party library	License	Project URL
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html*	https://www.oracle.com/index.html
ParaType Free Font	https://www.paratype.ru/public/pt_openlicense_eng.asp*	https://www.paratype.ru
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
script.aculo.us scriptaculous.js	https://madrobby.github.io/scriptaculous/license/*	http://script.aculo.us/
slt	MIT License**	https://code.google.com/archive/p/slt
SQLite	Public Domain https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	https://www.zlib.net/zlib_license.html*	https://www.zlib.net/

*—license texts are listed below.

**—text of basic licenses you can find at the following:

License	Address
Common Public License	https://opensource.org/licenses/cpl1.0.php
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Microsoft Public License	https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/licenses/mit-license.php

License	Address
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/
3-Clause BSD License	https://opensource.org/licenses/BSD-3-Clause

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. C-ares

```
Copyright (c) 2007 - 2018, Daniel Stenberg with many contributors, see AUTHORS file.

Copyright 1998 by the Massachusetts Institute of Technology.

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 appear in
all copies and that both that copyright notice and this permission notice appear in supporting
documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior permission. M.I.T. makes no
representations about the suitability of this software for any purpose. It is provided "as is"
without express or implied warranty.
```

M3. Curl

```
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.
```

M4. ICU

```
Copyright © 1991-2018 Unicode, Inc. All rights reserved.

Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data
files and any associated documentation (the "Data Files") or Unicode software and any associated
documentation (the "Software") to deal in the Data Files or Software without restriction,
including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or
sell copies of the Data Files or Software, and to permit persons to whom the Data Files or
Software are furnished to do so, provided that either (a) this copyright and permission notice
appear with all copies of the Data Files or Software, or (b) this copyright and permission
notice appear in associated Documentation.

THE DATA FILES AND SOFTWARE ARE 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 COPYRIGHT
HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR
CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM 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 THE DATA FILES OR 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 these Data Files or
Software without prior written authorization of the copyright holder.
```

M5. GCC runtime libraries—exception

```
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.
```

M6. Jemalloc

```
Unless otherwise specified, files in the jemalloc source distribution are subject to the
following license:

--------------------------------------------------------------------------------

Copyright (C) 2002-2018 Jason Evans <jasone@canonware.com>.

All rights reserved.

Copyright (C) 2007-2012 Mozilla Foundation.  All rights reserved.

Copyright (C) 2009-2018 Facebook, 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(s), this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice(s), 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 COPYRIGHT HOLDER(S) ``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(S) 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.

--------------------------------------------------------------------------------
```

M7. Leaflet

```
Copyright (c) 2010-2018, Vladimir Agafonkin
Copyright (c) 2010-2011, CloudMade

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 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 HOLDER 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.
```

M8. Libpng

```
If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.32, August 24, 2017 are Copyright (c) 2000-2002,
2004, 2006-2017 Glenn Randers-Pehrson, are derived from libpng-1.0.6, and are distributed
according to the same disclaimer and license as libpng-1.0.6 with the following individuals
added to the list of Contributing Authors:

   Simon-Pierre Cadieux

   Eric S. Raymond

   Mans Rullgard

   Cosmin Truta

   Gilles Vollant

   James Yu

   Mandar Sahastrabuddhe

   Google Inc.

   Vadim Barkov

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against
infringement.  There is no warranty that our efforts or the library will fulfill any of your
particular purposes or needs.  This library is provided with all faults, and the entire risk of
satisfactory quality, performance, accuracy, and effort is with the user.

Some files in the "contrib" directory and some configure-generated files that are distributed
with libpng have other copyright owners and are released under other open source licenses.
```

```
libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998-2000
Glenn Randers-Pehrson, are derived from libpng-0.96, and are distributed according to the same
disclaimer and license as libpng-0.96, with the following individuals added to the list of
Contributing Authors:

   Tom Lane

   Glenn Randers-Pehrson

   Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996-1997 Andreas
Dilger, are derived from libpng-0.88, and are distributed according to the same disclaimer and
license as libpng-0.88, with the following individuals added to the list of Contributing
Authors:

   John Bowler

   Kevin Bracey

   Sam Bushell

   Magnus Holmgren

   Greg Roelofs

   Tom Tanner

Some files in the "scripts" directory have other copyright owners but are released under this
license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995-1996 Guy Eric
Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the
following set of individuals:

   Andreas Dilger

   Dave Martindale

   Guy Eric Schalnat

   Paul Schmidt

   Tim Wegner

The PNG Reference Library is supplied "AS IS".  The Contributing Authors and Group 42, Inc.
disclaim all warranties, expressed or implied, including, without limitation, the warranties of
merchantability and of fitness for any purpose.  The Contributing Authors and Group 42, Inc.
assume no liability for direct, indirect, incidental, special, exemplary, or consequential
damages, which may result from the use of the PNG Reference Library, even if advised of the
possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions
hereof, for any purpose, without fee, subject to the following restrictions:

  1. The origin of this source code must not be misrepresented.

  2. Altered versions must be plainly marked as such and must not be misrepresented as being the
original source.

  3. This Copyright notice may not be removed or altered from any source or altered source
distribution.
```

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

April 1, 2017

M9. 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 $

M10. Libssh2

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>

Copyright (c) 2006-2007 The Written Word, Inc.

Copyright (c) 2007 Eli Fant <elifantu@mail.ru>

Copyright (c) 2009-2014 Daniel Stenberg

Copyright (C) 2008, 2009 Simon Josefsson

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 copyright holder nor the names of any other 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.
```

M11. Linenoise NG

linenoise

```
Copyright (c) 2010, Salvatore Sanfilippo <antirez at gmail dot com>

Copyright (c) 2010, Pieter Noordhuis <pcnoordhuis at gmail dot com>

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 Redis 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 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.
```

wcwidth

```
Markus Kuhn -- 2007-05-26 (Unicode 5.0)
```

```
Permission to use, copy, modify, and distribute this software for any purpose and without fee is
hereby granted. The author disclaims all warranties with regard to this software.
```

ConvertUTF

```
Copyright 2001-2004 Unicode, Inc.

 Disclaimer

 This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any
particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to
determine applicability of information provided. If this file has been purchased on magnetic or
optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective
media within 90 days of receipt.

 Limitations on Rights to Redistribute This Code

 Unicode, Inc. hereby grants the right to freely use the information supplied in this file in
the creation of products supporting the Unicode Standard, and to make copies of this file in any
form for internal or external distribution as long as this notice remains attached.
```

M12. 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.

M13. Noto Sans CJK

Copyright (c) <dates>, <Copyright Holder> (<URL|email>), with Reserved Font Name <Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>), with Reserved Font Name <additional Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>).

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:

http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

```
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE
AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE
COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL,
SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT
OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER
DEALINGS IN THE FONT SOFTWARE.
```

M14. 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.
```

M15. OpenSSL

```
Copyright (c) 1998-2018 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 licence 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 licence [including the GNU Public Licence.]
```

M16. 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

M17. ParaType Free Font

LICENSING AGREEMENT

for the fonts with Original Name: PT Sans, PT Serif, PT Mono

Version 1.3 - January 20, 2012

GRANT OF LICENSE

ParaType Ltd grants you the right to use, copy, modify the fonts and distribute modified and unmodified copies of the fonts by any means, including placing on Web servers for free downloading, embedding in documents and Web pages, bundling with commercial and non commercial products, if it does not conflict with the conditions listed below:

- You may bundle the fonts with commercial software, but you may not sell the fonts by themselves. They are free.

- You may distribute the fonts in modified or unmodified versions only together with this Licensing Agreement and with above copyright notice. You have no right to modify the text of Licensing Agreement. It can be placed in a separate text file or inserted into the font file, but it must be easily viewed by users.

- You may not distribute modified version of the font under the Original name or a combination of Original name with any other words without explicit written permission from ParaType.

TERMINATION & TERRITORY

This license has no limits on time and territory, but it becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL PARATYPE BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

ParaType Ltd

M18. PCRE

```
PCRE2 is a library of functions to support regular expressions whose syntax and semantics are as
close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified below,
with one exemption for certain binary redistributions. The documentation for PCRE2, supplied in
the "doc" directory, is distributed under the same terms as the software itself. The data in the
testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the
distribution is a just-in-time compiler that can be used to optimize pattern matching. This is
an optional feature 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) 1997-2018 University of Cambridge

All rights reserved.

PCRE2 JUST-IN-TIME COMPILATION SUPPORT

--------------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2010-2018 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) 2009-2018 Zoltan Herczeg

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 notices, this list of conditions and the following disclaimer.

 * Redistributions in binary form must reproduce the above copyright notices, 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 names of any 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.

EXEMPTION FOR BINARY LIBRARY-LIKE PACKAGES

The second condition in the BSD licence (covering binary redistributions) does not apply all the way down a chain of software. If binary package A includes PCRE2, it must respect the condition, but if package B is software that includes package A, the condition is not imposed on package B unless it uses PCRE2 independently.

M19. Script.aculo.us

Copyright © 2005-2008 Thomas Fuchs (http://script.aculo.us, http://mir.aculo.us)

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.

M20. Zlib

zlib.h -- interface of the 'zlib' general purpose compression library

```
  version 1.2.11, January 15th, 2017

  Copyright (C) 1995-2017 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
```

Chapter 3: Frequently Asked Questions

Moving Dr.Web Server to Another Computer (under Windows OS)

After moving Dr.Web 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.

Procedure of how to start and stop Dr.Web Server is described in the **Administrator Manual**, p. Start and Stop Dr.Web Server.

To transfer Dr.Web Server (for the similar Dr.Web Server versions) under Windows OS

1. Stop Dr.Web Server.
2. Run `drwcsd.exe` using the `modexecdb database-export` 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" -log=drwcsd.log modexecdb
database-export <full_filename>
```

3. Backup the `C:\Program Files\DrWeb Server\etc` folder.
4. Remove the Dr.Web Server software.
5. Install the new Dr.Web Server (empty, with the new DB) at the necessary computer. Stop Dr.Web 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.
7. Run `drwcsd.exe` using the `modexecdb database-import` 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" -log=drwcsd.log modexecdb
database-import <full_filename>
```

8. Start 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 Dr.Web Server by an old DB file from the previous version of Dr.Web Server.

To transfer Dr.Web Server (for the different Dr.Web Server versions) under Windows OS

1. 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.
4. Remove the Dr.Web Server software.
5. Install the new Dr.Web Server (empty, with the new DB) at the necessary computer. Stop Dr.Web 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.
7. Restore the DB on new Dr.Web Server and specify the path to the DB in the `drwcsd.conf` configuration file.
8. Run `drwcsd.exe` using the `modexecdb database-upgrade` switch to upgrade the database. The full command line (for Windows) looks as follows:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log modexecdb
   database-upgrade
   ```

9. Start 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 Dr.Web Server address is set via the Control Center, but not in the Agent settings at the station, keep both Dr.Web Servers operating till the procedure is completed.

1. Transfer Dr.Web Server according to the corresponding procedure, described above.
2. For all Agents, which are served by transferred Dr.Web Server, specify the address of the new Dr.Web 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 Dr.Web Server address is set via the Control Center, but not in the Agent settings at the station, on both Dr.Web Servers in the Agent settings, the new Dr.Web Server IP address must be specified.
3. Wait until all Agents connect to the new Dr.Web Server. After this, you can remove the old Dr.Web Server.

Connecting Dr.Web Agent to Other Dr.Web Server

You can connect the Agent to another Dr.Web 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 Dr.Web 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 Dr.Web Server. If you do not have these permissions, you can reconnect to other Dr.Web Server locally on the station only after removing installed Agent and installing the new Agent with the new Dr.Web 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 Dr.Web Server, allow the stations with incorrect authorization parameters to request new authorization parameters as being newbies. For this, in the Control Center, 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 Dr.Web 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 Dr.Web Server to which the Agent is connected, set the parameters of the new Dr.Web Server. For this, in the main menu of the Control Center, select the **Anti-Virus Network** item → select the required station (or the group for reconnecting all the stations of this group) in the hierarchical list of the network → in the control menu, select the **Connection settings** item:

   a) If the new Dr.Web Server certificate does not match the previous Dr.Web Server certificate, set the path to the new Dr.Web Server certificate in the **Certificate** field.

   b) Set the new Dr.Web Server address in the **Server** field.

   c) Click **Save**.

To reconnect Dr.Web Agent to another Dr.Web Server directly at station

1. Set the new Dr.Web Server parameters in the Agent settings. For this, in the context menu of the Agent icon, select **Security Center** → click the lock 🔒 (if it is not open yet) to get access to advanced settings → the ⚙ button to access the settings → the **Server** item → the **Connection parameters** section → the **Change settings** button:

   a) If the new Dr.Web Server certificate does not match the previous Dr.Web Server certificate, set the path to the new Dr.Web Server certificate using the **List of certificates** button.

   b) Set the corresponding parameters of the new Dr.Web Server using the **Add** button.

2. Make the station a newbie (reset the authorization parameters on Dr.Web Server). For this, in the connection settings section from the step 1, click the following: the **Station connection parameters** button → the **Reset the parameters and connect as a newbie** button → the **Reset the parameters** button.

   If you already know the ID and the password to connect the new Dr.Web 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

Procedure of how to start and stop Dr.Web Server is described in the **Administrator Manual**, p. Start and Stop Dr.Web Server.

1. Stop Dr.Web Server.
2. Run `drwcsd.exe` using the `modexecdb database-export` 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 -log=drwcsd.log modexecdb database-export 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`.

   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, connect Dr.Web Security Control Center to Dr.Web Server and configure Dr.Web Server to use a different DBMS. Cancel the Dr.Web Server restart.
4. Stop Dr.Web Server.
5. Delete the database file.
6. Run `drwcsd.exe` using the `modexecdb database-init` 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 -log=drwcsd.log modexecdb database-init D:\Keys\agent.key
   <password>
   ```

   It is presumed that Dr.Web Server is installed to the `C:\Program Files\DrWeb Server` folder and `agent.key` resides in `D:\Keys`.

   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"
   ```

7. Run `drwcsd.exe` using the `modexecdb database-import` 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 -log=drwcsd.log modexecdb database-import D:\esbase.es
```

8. Start Dr.Web Server.

For UNIX OS

1. Stop Dr.Web Server using the script

   - for **Linux** OS:

   ```
   /etc/init.d/drwcsd stop
   ```

   - for **FreeBSD** OS:

   ```
   /usr/local/etc/rc.d/drwcsd stop
   ```

   or via Dr.Web Security Control Center.

2. Start Dr.Web Server with the `modexecdb database-export` switch to export the database to a file. The command line from the Dr.Web Server installation folder will look as follows:

   - for **Linux** OS:

   ```
   /etc/init.d/drwcsd -log=drwcsd.log modexecdb database-
   export /var/esbase.es
   ```

   - for **FreeBSD** OS:

   ```
   /usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-
   export /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:

   ```
   /etc/init.d/drwcsd start
   ```

   - for **FreeBSD** OS:

   ```
   /usr/local/etc/rc.d/drwcsd start
   ```

   connect Dr.Web Security Control Center to Dr.Web Server and configure Dr.Web Server to use another database through Dr.Web Security Control Center menu: **Administration** → **Dr.Web Server configuration** → **Database** tab.

   You can also reconfigure Dr.Web Server to use another database/DBMS by editing the Dr.Web 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 Dr.Web Server. Reject restarting.

4. Stop Dr.Web Server (see step 1).
5. Delete the database file.
6. Run `drwcsd` using the `modexecdb database-init` switch to initialize a new database. The command line will look as follows:
   - for **Linux** OS:

   ```
   /etc/init.d/drwcsd -log=drwcsd.log modexecdb database-init
   ```

   - for **FreeBSD** OS:

   ```
   /usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-init
   ```

7. Run `drwcsd` using the `modexecdb database-import` switch to import the database from a file. The command line will look as follows:
   - for **Linux** OS:

   ```
   /etc/init.d/drwcsd -log=drwcsd.log modexecdb database-
   import /var/esbase.es
   ```

   - for **FreeBSD** OS:

   ```
   /usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-
   import /var/esbase.es
   ```

8. Start Dr.Web Server (see step 3).

If you want to change the parameters at Dr.Web Server start (for example, specify the Dr.Web 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
```

- for **Linux** OS:

```
/etc/init.d/drwcsd
```

Restoring the Database of Dr.Web Enterprise Security Suite

During the operation, Dr.Web Server regularly stores backup copies of important information: license keys, database contents, encryption private key, Dr.Web Server configuration and Control Center configuration.

The backup files are stored in the following folders:

- for **Windows** OS: <*installation_drive*>`:\DrWeb Backup`
- for **Linux** OS: `/var/opt/drwcs/backup`
- for **FreeBSD** OS: `/var/drwcs/backup`

To perform the back up, a daily task is included into the Dr.Web Server schedule. If such task is missing in the schedule, it is recommended to create it.

All files in the backup except the database contents, are ready to use. The database backup copy is stored in the `.gz` format compatible with `gzip` and other archivers. The database contents can be imported from the backup copy to another database of Dr.Web Server using the `modexecdb database-import` command, thus restore the data.

> To restore the database you can also use a backup created manually by administrator via the Control Center in the **Administration** → **Database management** → **Export** (for the **Export entire database** mode only).

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 Dr.Web Server of the same major version as the version of Dr.Web Server that you use for restoring.
>
> **For example:**
>
> - You can restore DB from the backup created via Dr.Web Server of 13 version using Dr.Web Server of 13 version only.
> - You cannot restore DB from the backup created via Dr.Web Server of 6 version using Dr.Web Server of 13 version.

If DB has been corrupted for some reasons during the Dr.Web Server upgrade from previous versions to 13.0 version, do the following:

1. Remove the Dr.Web Server software of the 13.0 version. Backup copies of files, used by Dr.Web Server, will be stored automatically.
2. Install Dr.Web 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 Dr.Web Server files except the DB file.

Create a new DB during the Dr.Web Server installation.

3. Restore DB from the backup according to general rules (see procedures below).
4. Disable the Agent, Dr.Web Server and the Network Installer protocols in the Dr.Web 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 Dr.Web Server to the 13.0 version according to general rules (see **Administrator Manual**, p. Updating Dr.Web Enterprise Security Suite Software and Its Components).
6. Enable the Agent, Dr.Web Server and the Network Installer protocols, disabled at the step 4.

For Windows OS

> Procedure of how to start and stop Dr.Web Server is described in the **Administrator Manual**, p. Start and Stop Dr.Web Server.

To restore DB from backup

1. Stop Dr.Web Server if it is running.
2. Import the content of the database from the correspondent backup file. The command line will look as follows:

   - for Dr.Web Server prior to version 13

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log importdb "<path_to_the_backup_file>\database.gz"
   ```

   - for Dr.Web Server version 13 and later

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log modexecdb database-import
   "<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.

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.
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:

- for Dr.Web Server prior to version 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log initdb D:\Keys\agent.key - - <password>
```

- for Dr.Web Server version 13 and later

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-init D:\Keys\agent.key
<password>
```

The command must be entered in a single line (see also `drwcsd` command format with the `modexecdb database-init` switch at the Appendix H3.3. Database Commands). It is presumed that Dr.Web Server is installed to the `C:\Program Files\DrWeb Server` folder and `agent.key` license key is located in `D:\Keys`.

c) Once this command is executed, a new `database.sqlite` will be generated in the `var` subfolder of Dr.Web Server installation folder.

2.2. For the external DB: clean up the DB using `cleandb` (for Dr.Web Server prior to version 13) or `modexecdb database-clean` (for Dr.Web Server version 13 and later) command (see Appendix H3.3. Database Commands).

3. Import the content of the database from the correspondent backup file. The command line will look as follows:

- for Dr.Web Server prior to version 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log importdb "<path_to_the_backup_file>\database.gz"
```

- for Dr.Web Server version 13 and later

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log modexecdb database-import
"<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.

4. Start Dr.Web Server.

For UNIX OS

1. Stop Dr.Web Server (if it is running):

- for **Linux** OS:

```
/etc/init.d/drwcsd stop
```

- for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd stop
```

2. Remove `database.sqlite` from the following subfolder of the Dr.Web Server installation folder:

   - for **Linux** OS: `/var/opt/drwcs/`
   - for **FreeBSD** OS: `/var/drwcs/`

> ! To clean an external DB, use `cleandb` (for Dr.Web Server prior to version 13) or `modexecdb database-clean` (for Dr.Web Server version 13 and later) command (see Appendix H3.3. Database Commands).

3. Initialize the Dr.Web Server database. The command will look as follows:

   - for **Linux** OS:
     - for Dr.Web Server prior to version 13

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

     - for Dr.Web Server version 13 and later

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-init
```

   - for **FreeBSD** OS:
     - for Dr.Web Server prior to version 13

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

     - for Dr.Web Server version 13 and later

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-init
```

4. Once this command is executed, a new `database.sqlite` database will be generated in the `var` subfolder of Dr.Web Server installation folder.

5. Import the content of the database from the correspondent backup file. The command line will look as follows:

   - for **Linux** OS:
     - for Dr.Web Server prior to version 13

```
/etc/init.d/drwcsd -log=drwcsd.log importdb
"<path_to_the_backup_file>/database.gz"
```

     - for Dr.Web Server version 13 and later

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-import
"<path_to_the_backup_file>/database.gz"
```

- for **FreeBSD** OS:
  - for Dr.Web Server prior to version 13

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb
"<path_to_the_backup_file>/database.gz"
```

  - for Dr.Web Server version 13 and later

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-import
"<path_to_the_backup_file>/database.gz"
```

6. Start Dr.Web Server:

- for **Linux** OS:

```
/etc/init.d/drwcsd start
```

- for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd start
```

If you want to run the script with parameters (e.g., set the Dr.Web Server installation directory and etc.), you must make all changes in the start script:

- for FreeBSD OS: `/usr/local/etc/rc.d/drwcsd`
- for Linux OS: `/etc/init.d/drwcsd`

If you need to change the log level of detail of Dr.Web Server, use the `local.conf` file:

- for Linux OS: `/var/opt/drwcs/etc/local.conf`;
- for FreeBSD OS: `/var/drwcs/etc/local.conf`.

If some Agents were installed after the last backup had been made, they will not be connected to Dr.Web Server after the database has been restored from the backup. You should remotely reset them to the newbie mode. In the **Administrating → Dr.Web Server configuration** on the **General** tab, set the **Reset unauthorized to newbie** flag and in the **Newbies registration mode** drop-down list, select **Allow access automatically**. Click **Save** and restart Dr.Web Server.

After all stations will be successfully connected to the new Dr.Web Server, change these Dr.Web Server settings to the settings adopted according to the policy of your company.

As soon as the database is restored from the backup it is recommended to connect Dr.Web Security Control Center to Dr.Web 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.

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 Dr.Web 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 Dr.Web 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 which 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.

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.

To install Dr.Web Agent 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.

Restoring the Anti-virus Network after Dr.Web Server Failure

In case Dr.Web Server fatal failure, it is recommended to use the following procedures to restore anti-virus network operability without reinstalling the Agents on stations.

> Meant, the new Dr.Web Server will be installed on a computer with the same IP address and DNS name.

Restoring from Dr.Web Server Backup

During the operation, Dr.Web Server regularly stores backup copies of important information: license keys, database contents, encryption private key, Dr.Web Server configuration and Control Center configuration.

The backup files are stored in the following folders:

- for **Windows** OS: <*installation_drive*>`:\DrWeb Backup`
- for **Linux** OS: `/var/opt/drwcs/backup`
- for **FreeBSD** OS: `/var/drwcs/backup`

To perform the back up, a daily task is included into the Dr.Web Server schedule. If such task is missing in the schedule, it is recommended to create it.

All files in the backup except the database contents, are ready to use. The database backup copy is stored in the `.gz` format compatible with `gzip` and other archivers. The database contents can be imported from the backup copy to another database of Dr.Web Server using the `modexecdb database-import-and-upgrade` command, thus restore the data.

> To restore the database you can also use a backup created manually by administrator via the Control Center in the **Administration** → **Database management** → **Export** (for the **Export entire database** mode only).

It is also recommended to store copies of created backups and other important files on another computer. Thus, you will be able to avoid data loss should the computer, on which Dr.Web Server is installed, be damaged, and to fully restore the data and the functionality of Dr.Web Server. If license keys are lost, they may be requested once again, as specified in **Administrator Manual**, p. Licensing.

To restore Dr.Web Server after the failure if the backup is available

1. Choose a computer to install the new Dr.Web Server. Isolate this computer from operating Agents: disconnect it from the network in which the Agents are installed or temporarily change its IP address, or use any other method you mostly prefer.
2. Install the new Dr.Web Server.

3. In the **Administrating** → **License manager** section, add the license key from the previous Dr.Web Server installation and propagate it on corresponding groups, particularly on the **Everyone** group. The step is obligatory if the license key was not set during the Dr.Web Server installation.

4. Update repository of the installed Dr.Web Server from the GUS:

   a) Open the **Administrating** → **Repository state** section of the Control Center.

   b) Click the **Check for updates** button to check whether updates to all of the products are available on the GUS servers and download updates, if any.

5. If new versions of the Dr.Web Server software are available, perform the update to the latest version:

   a) Open **Administrating** → **Dr.Web Server** section of the Control Center.

   b) To open the Dr.Web Server versions list, click the current version of Dr.Web Server or click the **Versions list** button. This opens the **Dr.Web Server Updates** section with the list of available updates and backups of Dr.Web Server.

   c) To update the Dr.Web Server software, set the option next to the last version in the **All versions** list. Click **Save**.

   d) Wait for the completion of the Dr.Web Server update process.

6. Stop Dr.Web Server.

7. Replace the Dr.Web Server critical data with the saved ones from the backup:

Operating system	Configuration files
Windows	`etc` in the Dr.Web Server installation folder
Linux	`/var/opt/drwcs/etc`
FreeBSD	`/var/drwcs/etc`

8. Configure the database.

   a) External database:

   No more actions to connect the database to Dr.Web Server are required (as long as the Dr.Web Server configuration file has been saved).

   If the version of Dr.Web Server installed from the last updates is later than the version of the lost Dr.Web Server, update the external database via the `modexecdb database-upgrade` command:

   - for Windows OS:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log
modexecdb database-upgrade
```

   - for Linux OS:

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-upgrade
```

- for FreeBSD OS:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-upgrade
```

b) Backup of external or embedded database:

For the external database, preliminary clean it up via the `modexecdb database-clean` command (see Appendix H3.3. Database Commands).

Import the database content from the corresponding backup file with database format updating to the installed Dr.Web Server version using the `modexecdb database-import-and-upgrade` command:

- 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 -log=drwcsd.log modexecdb database-import-and-upgrade
"<path_to_the_backup_file>\database.gz"
```

- for Linux OS:

```
/etc/init.d/drwcsd -log=drwcsd.log modexecdb database-import-and-
upgrade "<path_to_the_backup_file>/database.gz"
```

- for FreeBSD OS:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log modexecdb database-import-
and-upgrade "<path_to_the_backup_file>/database.gz"
```

For all replaced files assign the same permissions as those set at the previous (lost) installation of Dr.Web Server.

For UNIX system-based OS: `rw` for `drwcs:drwcs`.

9. Start Dr.Web Server.
10. Make sure that data from the database backup is save and actual: the Agent settings, anti-virus network tree state and etc.
11. Restore the Dr.Web Server accessibility for the Agents according to the Dr.Web Server isolation way selected on step 1.

If some Agents were installed after the last backup had been made, they will not be connected to Dr.Web Server after the database has been restored from the backup. You should remotely reset them to the newbie mode. In the **Administrating → Dr.Web Server configuration** on the **General** tab, set the **Reset unauthorized to newbie** flag and in the **Newbies registration mode** drop-down list, select **Allow access automatically**. Click **Save** and restart Dr.Web Server.

After all stations will be successfully connected to the new Dr.Web Server, change these Dr.Web Server settings to the settings adopted according to the policy of your company.

Restoring without Dr.Web Server Backup

To restore Dr.Web Server after the failure if no backup had been saved

1. Choose a computer to install the new Dr.Web Server. Isolate this computer from operating Agents: disconnect it from the network in which the Agents are installed or temporarily change its IP address, or use any other method you mostly prefer.
2. Install the new Dr.Web Server.
3. In the **Administrating → License manager** section, add the license key from the previous Dr.Web Server installation and propagate it on corresponding groups, particularly on the **Everyone** group. The step is obligatory if the license key was not set during the Dr.Web Server installation.
4. Update repository of the installed Dr.Web Server from the GUS:
   a) Open the **Administrating → Repository state** section of the Control Center.
   b) Click the **Check for updates** button to check whether updates to all of the products are available on the GUS servers and download updates, if any.
5. If new versions of the Dr.Web Server software are available, perform the update to the latest version:
   a) Open **Administrating → Dr.Web Server** section of the Control Center.
   b) To open the Dr.Web Server versions list, click the current version of Dr.Web Server or click the **Versions list** button. This opens the **Dr.Web Server Updates** section with the list of available updates and backups of Dr.Web Server.
   c) To update the Dr.Web Server software, set the option next to the last version in the **All versions** list. Click **Save**.
   d) Wait for the completion of the Dr.Web Server update process.
6. Change the stations connection settings in the Dr.Web Server configuration:
   a) Open **Administrating → Dr.Web Server configuration**.
   b) On the **General** tab, set the **Reset unauthorized to newbie** flag.
   c) On the **General** tab in the **Newbies registration mode** drop-down list, select **Allow access automatically**.
   d) Click **Save** and restart Dr.Web Server.
7. In the **Anti-virus Network** section of the Control Center, create user groups in the anti-virus network tree similarly with the previous version. If necessary, create automatic membership rules for stations in the created user groups.

8. If necessary, specify the Agent settings and the Dr.Web Server settings (except the temporary settings from the step 5) similarly with the previous version.
9. If necessary, change the repository settings in the **Administrating → Detailed repository configuration** section.
10. Restore the Dr.Web Server accessibility for the Agents according to the Dr.Web Server isolation way selected on step 1.
11. Replace the public encryption key on all stations of the network that are planned to connect to the new Dr.Web Server.
    - If the self-protection is enabled, copy to a station the public key created during the new Dr.Web Server installation and run the following command:

      ```
      es-service.exe -p <key>
      ```

      or

      ```
      es-service.exe --addpubkey=<key>
      ```

      As the <*key*>, specify the path to the public encryption key copied to a station.

      In a result, the public key will be copied to the Agent installation folder. By default, it is the `%ProgramFiles%\DrWeb` folder (for more details, see the Appendix H2. Dr.Web Agent for Windows).
    - If the self-protection is disabled on a station, you can take the public key created during the new Dr.Web Server installation and place it into the folder specified above.
12. After all stations will be successfully connected to the new Dr.Web Server, change the Dr.Web Server settings specified on step 5 to the settings adopted according to the policy of your company.

Managing the Logging Level of Dr.Web Server for Windows OS

You can change the level of logging detail for Dr.Web Server under Windows OS by one of the following ways:

- Using the **Dr.Web Server configuration → Log** section of the Control Center.

  This method is preferred. In the **Log** section, you can specify any allowed level of logging detail for Dr.Web Server, and also some other settings.

  Detailed information is given in the **Administrator Manual**, in the Dr.Web Server configuration → Log section.
- Using the console command:

  ```
  drwcsd [<switches>] install
  ```

  You can specify any allowed level of logging detail for Dr.Web Server via the `--verbosity` switch.

Detailed information on command line switches for the Dr.Web Server management is given in the H3.8. The Description of Switches section.

Command example to set the **Detailed** logging level:

```
drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
\Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb Server\var"
--verbosity=ALL --log=drwcsd.log --rotate=10,50m install
```

The other switches are mandatory, particularly, if you have redefined standard paths of the Dr.Web Server installation and working folders.

After the log verbosity level has been changed, restart Dr.Web Server:

```
drwcsd restart
```

- Using the commands in the **Start** main menu of Windows OS.

  At this, only two possible levels of logging detail are available: **Detailed** or **Default**:

  a) **Programs** → **Dr.Web Server control** → **Detailed logging**
  or
  Programs → **Dr.Web Server control** → **Default logging**

  b) **Programs** → **Dr.Web Server control** → **Restart**.

Automatic Location of Stations under Android OS

Dr.Web Enterprise Security Suite allows automatic providing an administrator with information about geographic location of protected mobile devices under Android OS.

To locate a mobile device

1. Configure the transmission of the information on a mobile device location to Dr.Web Server:

   a) In Dr.Web Security Control Center, in the **Anti-virus network** section, in the network tree, select the necessary station or the group of stations under Android OS.

   b) Select the **Dr.Web for Android** item in the control menu.

   c) On the **General** tab, set the **Track location** flag. In the **Period of coordinates transmission** drop-down list, select a value according to which the device location data will be updated.

   d) Save the changes.

2. Automatic location tracking is performed by one of the following ways:

   - If location providers (GPS, mobile networks) are enabled on a user device and the signal is stable, the location is monitored by the means of a mobile device itself.
   - If location providers (GPS, mobile networks) are disabled on a user device or there is no GPS signal, Dr.Web Enterprise Security Suite provides the feature to use the Yandex.Locator technology to locate a mobile device on the coordinates of the mobile communication towers (GSM, 3D, LTE) and WiFi ID.

To configure the Yandex.Locator technology, you must activate and set up the **Yandex.Locator Extension**:

a) Get the API key on Yandex company website at https://yandex.ru/dev/locator/keys/get/.

b) In Dr.Web Security Control Center, in the **Administration** → **Dr.Web Server configuration** → **Modules** section, set the **Yandex.Locator Extension** flag.

c) In the **API key** field, specify the key received on the step a).

d) Save the changes and restart Dr.Web Server.

WiFi ID can only be used on mobile devices running Android 5.1 or earlier.

3. To view a station location in Dr.Web Security Control Center:

a) In the **Anti-virus network** section, in the network tree, select the station for which the corresponding settings were specified at step 1.

b) In the station properties, in the **Location** section, geographic coordinates received from a mobile devise will be filled automatically.

c) Click **Show on map** to view geographic location on a mobile device on OpenStreetMap according to the received coordinates.

Examples of Accessing Dr.Web Server Database

Further texts contain examples of SQL queries to PostgreSQL database. Queries to other databases may contain some differences due to the features of the database itself and the subtleties of its use.

> The capabilities of SQL do not allow to take into consideration the hierarchy of groups and stations.

To appeal the database directly

1. Open the Control Center of your Dr.Web Server.
2. Go to the **Administration** → **SQL console** section.
3. Type the necessary SQL query. Queries examples are given below.
4. Click **Execute**.

Examples of SQL Queries

1. Find stations with Windows Server OS installed and whose virus databases are older than 2019.07.04-00:00:00 UTC (12.0).

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform =(
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. Find stations that have records with the **High** and **Maximal** severity in the **Anti-virus network** → **Statistics** → **Status** section.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
    FROM
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. Get the correspondence between statuses and the number of stations with these statuses.

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. Get the top 10 of threats detected from 2019.06.01 to 2019.07.01 on stations included into the group with the '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5' identifier or in any groups nested in it.

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. Get the top 10 infected stations.

```
SELECT
  Station,
  Grp,
  Num
FROM
  (
    SELECT
      stations.id,
      groups_list.id,
      stations.name Station,
      groups_list.name Grp,
      COUNT(stations.id) Num
    FROM
      station_infection
      INNER JOIN stations ON station_infection.id = stations.id
      INNER JOIN groups_list ON groups_list.id = stations.gid
    GROUP BY
      stations.id,
      groups_list.id,
      stations.name,
      groups_list.name
    ORDER BY
      Num DESC
    LIMIT
      10
  ) AS t;
```

6. Remove membership for all stations from user groups that are not primary for these stations.

```
DELETE FROM
  station_groups;
INSERT INTO station_groups(sid, gid)
SELECT
  stations.id,
  groups_list.id
FROM
  stations
  INNER JOIN groups_list ON stations.gid = groups_list.id
  AND groups_list.type NOT IN(1, 4);
```

7. Fins object of the anti-virus network that contain the specified domain in the white list of the SpIDer Gate component personal settings.

```
SELECT
  stations.name Station
FROM
  station_cfg
  INNER JOIN stations ON stations.id = station_cfg.id
WHERE
  station_cfg.component = 38
  AND station_cfg.name = 'WhiteVirUrlList'
  AND station_cfg.value = 'domain.tld';
SELECT
  groups_list.name Grp
FROM
  group_cfg
  INNER JOIN groups_list ON groups_list.id = group_cfg.id
WHERE
  group_cfg.component = 38
  AND group_cfg.name = 'WhiteVirUrlList'
  AND group_cfg.value = 'domain.tld';
SELECT
  policy_list.name Policy
FROM
  policy_cfg
  INNER JOIN policy_list ON policy_list.id = policy_cfg.id
WHERE
  policy_cfg.component = 38
  AND policy_cfg.name = 'WhiteVirUrlList'
  AND policy_cfg.value = 'domain.tld';
```

8. Get the events of failed logins of administrators to the Control Center with corresponding authorization error codes.

```
SELECT
  admin_activity.login Login,
  admin_activity.address Address,
  activity_data.value ErrorCode,
  admin_activity.createtime EventTimestamp
FROM
  admin_activity
  INNER JOIN activity_data ON admin_activity.record = activity_data.record
WHERE
  admin_activity.oper = 10100
  AND admin_activity.status != 1
  AND activity_data.item = 'Error';
```

9. Find stations under Windows OS without necessary security fixes installed.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id NOT IN (
    SELECT
      station_env_kb.id
    FROM
      station_env_kb
      INNER JOIN stations ON stations.id = station_env_kb.id
    WHERE
      (
        CAST(stations.lastos AS INTEGER) & 2130706432
      )= 33554432
      AND station_env_kb.name IN (
        SELECT
          id
        FROM
          env_strings
        WHERE
          str IN(
            'KB4012212', 'KB4012213', 'KB4012214',
            'KB4012215', 'KB4012216', 'KB4012217',
            'KB4012598'
          )
      )
  );
```

Chapter 4: Trouble Shooting

Remote Installation Trouble Shooting

Principle of the installation:

1. Dr.Web Server connects to the `ADMIN$` resource at the remote station (`\\`<*remote_station*>`\ADMIN$\Temp`) and copies the network installer `drwinst.exe` that is located in the `webmin\install\windows` folder of the Dr.Web Server installation folder and SSL certificate `drwcsd-certificate.pem` located in the `etc` folder of the Dr.Web Server installation folder, to the `\\`<*remote_station*>`\ADMIN$\Temp` folder.
2. Dr.Web Server runs `drwinst.exe` file at the remote station with the command line switches according to the Control Center settings.

Successful installation requires the following on Dr.Web Server 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 assess 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 assess to the 455 port;

   c) limitations of remote assess 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` file and the `*.pub` public encryption key are available.

Dr.Web Security Control Center displays the external information (step and error code), which can help to diagnose the error reason.

The List of Dr.Web Agent Remote Installation Errors

Step	Error	Reason
Connecting via SMB to the <*host*> station	Invalid address of the <*host*> station	Station IP address that is specified for the Agent installation is not a valid IPv4/IPv6 address or conversion of DNS name to address has failed: no such DNS name or a name server is incorrectly configured.
	Error connecting via SMB to the <*host*> station	Unable to connect to a station via SMB. Possible reasons: • the server service is disabled on a station; • the 445 port is not available at the remote station, possible reasons: ▫ station is turned off; ▫ firewall blocks specified port; ▫ the OS at a remote station is not Windows OS. • sharing and security model for local accounts is not configured; • authorization server (domain controller) is not available; • unknown user name or bad password.
	Insufficient privileges to open the <*share*> shared resource at the <*host*> station	The `ADMIN$` resource does not exist on a remote station, or not enough privileges to open it.
Sending files to the <*host*> station	The <*path*> path in the <*share*> shared resource is not found on the <*host*> station	The `ADMIN$/TEMP` directory does not exist.
	Unable to create the <*path*> temporary folder in the <*share*> shared resource on the <*host*> station	Unable to create the temporary directory in `ADMIN$/TEMP`, e.g., not enough privileges to write.
	Unable to delete the <*path*> temporary folder in the <*share*> shared resource on the <*host*> station	Unable to delete the temporary directory in `ADMIN$/TEMP` after the procedure is complete. E.g., if the service was not completed, or someone opened a file in this directory.

Step	Error	Reason
	Unable to open the <*path*> file for reading on Dr.Web Server Unable to read the <*path*> file on Dr.Web Server	The installer file was not found on Dr.Web Server, or insufficient privileges are set on the installer file.
	Unable to open the <*path*> file for writing in the <*share*> shared folder on the <*host*> station Unable to write the <*path*> file in the <*share*> shared folder on the <*host*> station	Not enough privileges to read/write corresponding files or in the corresponding directories.
Creating service on the <*host*> station	Error connecting to the server service (srvsvc RPC) on the <*host*> station	Remote management of services is not available.
	Error connecting to SCM on the <*host*> station Unable to create the service on the <*host*> station Unable to start the service on the <*host*> station Unable to stop the service on the <*host*> station Unable to delete the service on the <*host*> station	Not enough privileges to control services.
Running service on the <*host*> station	Unable to get the service state on the <*host*> station	Possible SCM error.
	Installation timed out on the <*host*> station	The installer did not have time to install the Agent for the specified period. Possible reasons: a slow channel between the station and Dr.Web Server, not enough time to download necessary data.
	Unable to get the local path to the <*share*> shared resource on the <*host*> station	Unable to locate the path to the `ADMIN$` resource on the station.
	The service has faulted with an error on the <*host*> station.	The Agent installer errors.

Step	Error	Reason
	Completion state: <*share*>. Error code: <*rc*>.	

Resolving an Error of BFE during Dr.Web Agent for Windows Installation

For operation of some components of Dr.Web Anti-virus for Windows, Base Filtering Engine (BFE) service must be running. If this service is missing or damaged, Dr.Web Agent for Windows cannot be installed. Corruption or absence of BFE service can indicate security threats on the station.

If Dr.Web Agent for Windows installation attempt is failed with BFE error, you must perform the following actions:

1. Scan the station system using the CureNet! utility provided by Doctor Web company.

   You can request the demo version (diagnostics but not curing) of the utility here: https://download.drweb.com/curenet/.

   You can read the terms of use and the cost of the utility full version here: https://estore.drweb.com/utilities/.

2. Enable or restart BFE service. If you cannot restart BFE service or it is missing from the list of services, please contact Microsoft technical support.

3. Run Dr.Web Agent for Windows installer and perform the installation according to the general procedure given in the **Installation Manual**.

   If the problem still remains, please contact the Doctor Web technical support service.

Technical Support

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

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at https://forum.drweb.com/.

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

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

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

Keyword Index