

INFOWATCH

InfoWatch Device Monitor. Installation, Configuration and Administration Guide

04/04/2023

© JSC “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 4

2 Set of Documents 5

3 Hardware and Software Requirements 6

4 Installing InfoWatch Device Monitor 9

4.1 Deployment Scheme for InfoWatch Device Monitor 9

4.2 InfoWatch Device Monitor Server End Setup 12

4.2.1 Database Deployment Managed by Microsoft SQL Server DBMS 12

4.2.2 Database deployment managed by Oracle DBMS 13

Configuring InfoWatch Device Monitor connection to Oracle DBMS server 13

4.2.3 Database deployment managed by PostgreSQL DBMS 14

4.2.4 Server Setup Recommendations 14

4.2.5 InfoWatch Device Monitor Server End Installation Procedure 15

4.3 InfoWatch Device Monitor Agent Installation 24

4.3.1 Standard Agent Installation 26

Installing Device Monitor Agent on the computer with OS Microsoft Windows using cmd package containing installation parameters: 27

Installing Device Monitor Agent to on the computer with RED OS: 28

4.3.2 Agent Installation via Software Distribution Tools 28

5 Configuring InfoWatch Device Monitor Server 33

5.1 <applicationSettings> Section 34

5.2 <system.diagnostics> Section 42

5.3 Deleting Device Monitor temporary files 44

5.4 Configuring protection against guessing for Device Monitor 45

6 Updating InfoWatch Device Monitor 46

6.1 Updating InfoWatch Device Monitor Server End 46

6.2 Updating InfoWatch Device Monitor Agent 48

7 Uninstalling Device Monitor 50

7.1 Remove Agent Installed via Software Distribution Tools 51

8 Appendix A. Username and Password Recommendations 52

This guide contains information on how to install update remove and configure components of the module InfoWatch Device Monitor.

InfoWatch Device Monitor (also referred to as the Module or Device Monitor – software intended to intercept data.

1 Who Should Read this Guide

Information in this guide is intended for users who manage the System (perform the System configuration, analyze information objects, etc.).

This guide is intended for users familiar with the basics of Windows, RED OS and PostgreSQL DBMS.

2 Set of Documents

InfoWatch Device Monitor documentation package includes the following:

- "InfoWatch Device Monitor. Installation, configuration and administration Guide". The document describes how to install, update, uninstall and configure the Module.
- "InfoWatch Device Monitor. User Guide". The document describes how to work in InfoWatch Device Monitor.

Associated documentation for InfoWatch Traffic Monitor includes the following:

- «InfoWatch Traffic Monitor. Installation Guide». The document describes how to install, configure and uninstall InfoWatch Traffic Monitor (further referred to as Traffic Monitor).
- «InfoWatch Traffic Monitor. Administration Guide». The document describes how to administer the System (database, server).
- «InfoWatch Traffic Monitor. User Guide». The document describes how to work in InfoWatch Traffic Monitor (configuration setting, export/import of data, creating policies to process objects).
- «InfoWatch Traffic Monitor. Configuration Files Guide». Describes the content of the configuration files.

3 Hardware and Software Requirements

Hardware requirements for Traffic Monitor Server are defined based on the estimated load on the System and parameters of the network, where the System is installed. Therefore, the equipment specification is determined individually in each case.

Estimated minimal software and hardware requirements are listed in the following table. We strongly recommend you to make a detailed configuration computation with the assistance of InfoWatch experts or specialists of partner company from which you have purchased the product.

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor server				
Not less than 3 GB of free space for installation. You also need a space for data analysis, the size depends on server's load.	From 2 cores	From 2 GB	OS (x86 and x64 platforms are supported): • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019. Platform: • Microsoft .Net Framework 4.5.1. DBMS: • Oracle Database 19; • Microsoft SQL Server 2005, 2008, 2012, 2014, 2016, 2017, 2019 (Standard, Enterprise); • PostgreSQL version 13.	▪ Autostart for **iw_xapi_xapi** process should be enabled on TM server ▪ Local DNS is required to convert domain names into addresses ▪ FIPS mode should be disabled ▪ TLS 1.2 should be supported

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor Agent for workstations				
Not less than 1 GB free space required for installation. Also the free space is required for files temporary storage, which are to be sent for analysis.	From 2 cores	From 2,5 GB	OS: • [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • Microsoft Windows 11; • [1]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • RED OS 7.3.1.	• Local DNS is required to convert domain names into addresses • TLS 1.2 should be supported For the installation of the Device Monitor Agent version 7.6 and higher, the following versions of the RED OS kernel are supported: • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-5 • 5.15.72-1 (starting from version 7.7.1)
Device Monitor Management Console				
Not less than 35 MB	Same as for used OS	Same as for used OS	OS: • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016;	

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
			• Microsoft Windows Server 2019; • Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 and 8.1; • Microsoft Windows 10.	

Note!

[1] - marked operating systems require the following Microsoft updates: KB4474419, KB4490628. The System is intended to check the computer for bug fix before starting the installation and/or update.

Note:

You can install the System to the virtual environment: VMware, MS Hyper-V, or other virtualization systems.

Device Monitor agents' activity is supported within Microsoft RDS, Citrix XenApp 6.0, 7.6, 7.13, 7.14, and 7.15 LTSR virtualization environments.

4 Installing InfoWatch Device Monitor

Installation is performed in the following order:

1. InfoWatch Device Monitor Server End Setup.
   Server end consists of the following elements:
   - Database
   - Device Monitor Server
   - Device Monitor Management Console.
2. InfoWatch Device Monitor Agent Installation.
   Agent is installed on each computer that should be controlled by InfoWatch Device Monitor.

Before installation, make sure that environment where the System will be deployed matches software and hardware requirements (see "Hardware and Software Requirements").

Warning!

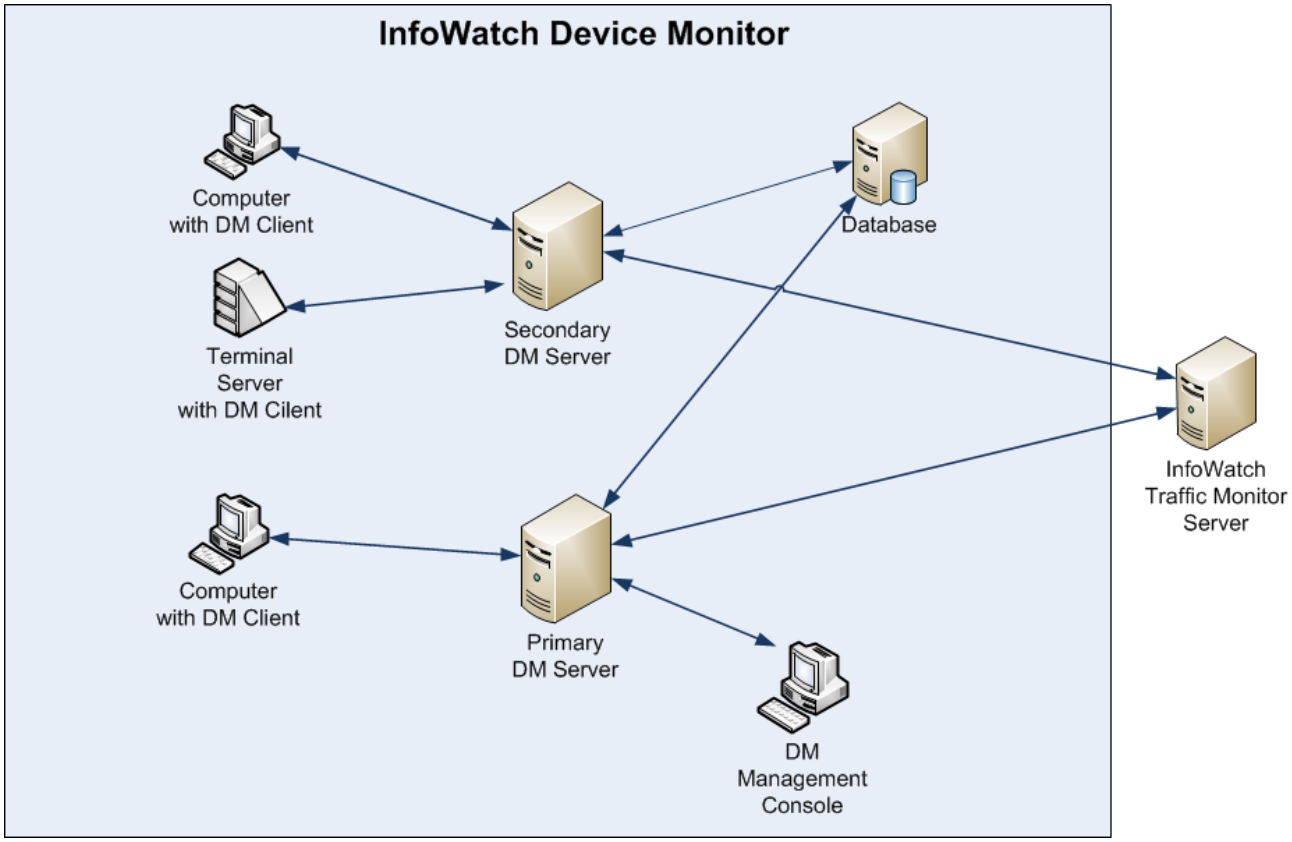
To ensure the correct operation and all the functionalities available Traffic Monitor and Device Monitor versions should comply. See more details about Device Monitor compatibility in the InfoWatchKnowledge Base article "Compatibility among the versions of TM, DM and Agents".

4.1 Deployment Scheme for InfoWatch Device Monitor

InfoWatch Device Monitor components are listed in the following table:

Component	Purpose
InfoWatch Device Monitor Client (InfoWatch device monitor client application, Agent)	Intercepting employees' actions on controlled computers
InfoWatch Device Monitor Server (InfoWatch Device monitor server, Server)	Configuring agents applications, retrieving data from agents and sending it to InfoWatch Traffic Monitor, distribution of deploy-agents to workstations
InfoWatch Device Monitor Database (database)	Storing data which is required for the operation of Device Monitor
InfoWatch Device Monitor Management Console (Management Console)	Managing Device Monitor
Distribution service	Getting and storing the new version of Agent's distibution kit
Servers Manager	Configuring roles and other attributes of Device Monitor servers

The following image illustrates interaction of Device Monitor components:



You can use clustering to enhance performance. The same database schema will be used by multiple servers to store and distribute shared security schema.

Server and database can be hosted on a single computer. To increase the performance, it is recommended that you should host the database and server on separate computers.

The Management Console can only connect to the main server. From the Management Console, you can manage all servers in the cluster.

InfoWatch DeviceMonitor is deployed and works as follows:

1. The **primary server** is installed first (see the document "*Infowatch Traffic Monitor. User Guide*", "InfoWatch Device Monitor Server Manager" article).
2. When you install the primary server, you should specify the server that will be used by the **database**: DBMS can be stored separately or together with the primary server.
3. During the installation of the primary server, a **database schema** is created, where the **security schema** and other Device Monitor parameters are stored.
4. You can install **secondary servers**, if needed, to balance the workload.
5. The **Management Console** can be installed on any computer. It connects to the primary server. The Management Console is used for configuring the security scheme according to the corporate security policy.
6. By default, the server with dstributive is installed together with **base Device Monitor server**, and has the storage with Agent distributive for the OS being used and platform.
7. Device Monitor Deploy-agents are distributed from **base server** to **workstations**. Then, the workstations download Agent distributive from the specified distribution points of the closest **distribution server**. Several workstations can download the distributive simultaneously.
8. Agents connect to any available Device Monitor Server via an encrypted channel with binding to the Server by the key, which is used for traffic encryption. Device Monitor agents ensure

implementation of security schemes; they also retrieve shadow copies and send them to Device Monitor Server.
9. Device Monitor Server retrieves updated versions of the security scheme from the database and distributes them to controlled workstations. Information about events that subject to a security scheme rule and files shadow copies are sent from controlled workstations to the Server. Information about the events is sent to the database. Shadow copies are sent to InfoWatch Traffic Monitor.

Example 1

1. An employee who works at a controlled workstation tries to get access to a controlled peripheral (for example, attempts to print a document on a USB printer).
2. The Agent checks if the employee has permissions to access the peripheral. If not, access is denied (in this case, the document will not be printed).

Printing operations on local and network printers are monitored by Print Monitor interceptor. Print task copies are sent to InfoWatch Monitor Traffic for analysis. Employees can print documents, only if they are allowed to access the printer (this is checked by Device Monitor interceptor).

Example 2

There is a rule in Device Monitor that monitors writing to PDF files on a removable device. According to the rule, during this operation, a shadow copy of the document is created.

1. An employee who works at a controlled workstation writes data to a file on a removable device (for example, copies a file to USB flash drive).
2. If writing to a removable device is successful, InfoWatch Device Monitor Agent generates an event and creates a shadow copy of the file.
3. If the creation of a shadow copy fails (for example, there is no free space on the hard drive), writing to file will be performed without creating a shadow copy (this will be specified in the event data).
4. The Agent transmits data (the event and the file shadow copy) to InfoWatch Device Monitor Server. If there is no connection to the Server, the data is stored on the computer. Once the connection is restored, the data will be sent to Server.
5. The Server sends data to InfoWatch Traffic Monitor for analysis. If no there is no connection to InfoWatch Traffic Monitor server, the data is stored on the computer. Once the connection is restored, the data will be sent to InfoWatch Traffic Monitor.

Any attempts to write to files on removable devices are monitored by File Monitor interceptor. Obtained data is then passed to InfoWatch Traffic Monitor for analysis. At the same time, access to removable devices is controlled by Device Monitor interceptor. Therefore, employees can write data to file on a removable device only if they have access to the device.

Example 3

There is a rule in Device Monitor that monitors DOC files. According to the rule, during this operation, a shadow copy of the document is created.

1. An employee who works at a controlled workstation sends a document to print.
2. If the print job is created successfully, InfoWatch Device Monitor Agent generates an event and creates a shadow copy of the printed document.
3. If the creation of a shadow copy fails (for example, there is no free space on hard drive), print operation will be performed without creating a shadow copy (this will be specified in the event data).
4. The Agent transmits data (the event and the file shadow copy) to InfoWatch Device Monitor Server. If there is no connection to the Server, the data is stored on the computer. Once the connection is restored, the data will be sent to Server.

5. The Server sends data to InfoWatch Traffic Monitor for analysis. If no there is no connection to InfoWatch Traffic Monitor server, the data is stored on the computer. Once the connection is restored, the data will be sent to InfoWatch Traffic Monitor.

4.2 InfoWatch Device Monitor Server End Setup

InfoWatch Device Monitor server end is installed with universal Setup Wizard.
Universal Setup Wizard disk is available on your System installation CD (Setup.Unified directory). This program lets you install all System components except the Agent: database, Device Monitor Server, and Management Console.
The InfoWatch Device Monitor system can use Microsoft SQL Server or Oracle DBMS or PostgreSQL for managing the database.
Management Console connects to the primary server.
For more information on installation, see:

- Database Deployment Managed by Microsoft SQL Server DBMS
- Database deployment managed by Oracle DBMS
- InfoWatch Device Monitor Server Setup
- InfoWatch Device Monitor Server End Installation Procedure

4.2.1 Database Deployment Managed by Microsoft SQL Server DBMS

You must install Microsoft .NET Framework 2.0 Service Pack 1 and Microsoft .NET Framework 4.0 or higher before launching database scheme generation on your computer.

Database generation account must be configured in advance. Account type depends on database server authentication. Microsoft SQL Server DBMS supports two types of authentication:

- **Windows authentication**. Authentication uses accounts within Windows domain. Authentication data is processed by Microsoft Windows security.
- **SQL Server built-in authentication**. Uses Microsoft SQL Server accounts. Authentication is carried out via DBMS.

> **Important!**
>
> To ensure satisfactory safety level, we strongly recommend that you use **Windows authentication** method.

If you are going to use Windows authentication method:

1. Make sure Windows domain contains only one account that you will use for database generation. This account must have local administrator privileges on the computer used for database generation. If necessary, create a new account.
2. Add the account to Microsoft SQL Server DBMS and select **Windows authentication**.
3. Assign **dbcreator** role to the account.

If you plan to use SQL Server built-in authentication method:

1. Create a new Microsoft SQL Server account. When configuring an account: select **SQL Server built-in**, enter user name and password.
2. Assign **dbcreator** role to the account.

Note:

Integrated account name and password are specified when configuring the database (see "InfoWatch Device Monitor Server End Installation Procedure", step 7).

4.2.2 Database deployment managed by Oracle DBMS

The following components should be installed on the computer before launching the database schema generation:

- Microsoft .NET Framework 4.5 pack
- Oracle DBMS client (only after Microsoft .NET Framework 4.5 packs have been installed)
- Oracle Database Provider for .NET (ODP.NET)

Important!

Enable this feature by selecting the corresponding field in the Custom installation type. Installation must be run under the administrator account.

Before you start creating a database scheme, make sure that **tnsnames.ora** file contains database server connection parameters (see "Configuring ORACLE DBMS connection").

Configuring InfoWatch Device Monitor connection to Oracle DBMS server

To ensure proper connection to Oracle DBMS server for each computer with Oracle DBMS client, you must specify connection options. Choose one of the two options described below.

Option 1. Configure tnsnames.ora file ([ORACLE_HOME]\network\admin)

Specify Oracle DBMS server connection settings. To do this, add the following entry to `tnsnames.ora` file:

```
tns_name =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = service_name)
)
)
```

Specify true values for the following parameters:

- `tns_name` – Oracle DBMS server alias;
- `host_name` – Oracle DBMS domain name or IP address;
- `port_number` – server port for listening to client connections;
- `service_name` – database service name.

Example of tnsnames.ora file:

```
IWDM =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
```

```
(SERVICE_NAME = orcl)
)
)
```

Important!

The `tnsnames.ora` file is format sensitive. If you copy an example to edit a file, make sure that the copied selection does not contain any blank strings.

Option 2. Specify TNS string representation from tnsnames.ora file as a database server.

Example of string representation

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=iwdm.infowatch.ru)(PORT=1521))
(CONNECT_DATA=(SERVER=dedicated)(SERVICE_NAME=iwtm)))
```

4.2.3 Database deployment managed by PostgreSQL DBMS

There are the following preliminary requirements for the computer, where the database creation is to be started from:

- OS Microsoft Windows Server 2008 R2/2012/2012 R2/2016/2019;
- Microsoft .NET Framework 4.5.2 pack.

Download PostgreSQL 13 from the official site and install it with default parameters.

When installing the application, postgres superuser is to be created, to which the password should be granted. The related information is to be available in the utility pgAdmin III in "Entrance roles" section, a part installation pack.

After PostgreSQL is installed, please open `postgresql.conf` configuration file and assign value 250 to `"max_connections"` parameter.

Note:

To increase the System's response speed it is recommended installing OS, InfoWatch Device Monitor server end and PostgreSQL SMDB on different hard drives.

4.2.4 Server Setup Recommendations

To enhance the performance of Device Monitor, we recommend that you should deploy the server and database on separate computers.

Device Monitor server and Device Monitor Agent should be installed in the same time zone. This will assure that the time of intercepted event is correct.

Important!

When deploying a multiple-server pool, each server must have the same InfoWatch Device Monitor server application version installed that is compatible with the appropriate up-to-date database.

While configuring the Server (see "InfoWatch Device Monitor Server End Installation Procedure"), you must specify the account that will be launching InfoWatch Device Monitor Server. Available options:

- **Local System**. Launch service from system account.
- **User**. Launch service from Windows domain account.

For Microsoft SQL Server DBMS database. If you select **Windows authentification** for database owner (see "Database deployment under Microsoft SQL Server DBMS"), while database and Server are on separate computers, select **User** variant.

Important!

It is not recommended to select Local System option. In this case, the user can obtain unlimited rights, which contradicts the security policy.

Create service account and grant write access to installation catalogue: `\Program Files\InfoWatch\Device Monitor\Server`

Windows domain account (**User**) must be configured in advance. To do this:

1. Allow the account to run process as a service:

- In the **Control Panel** open **Administration** > **Local security policy**.
- In the following dialog select **Local policies** > **Assign User Rights**.
- Double-click **Log on as service** in the right **Details** pane.
- On **Local security parameter** tab add the account.

- Add a new account to Microsoft SQL Server DBMS account list.
When setup finishes, allow the account to create new databases. When specifying database access permission, select **db_owner** role.

4.2.5 InfoWatch Device Monitor Server End Installation Procedure

Warning!

Before starting the installation, see "Installing InfoWatch Device Monitor ".

Warning!

When deploying a multiple-server pool, each of them must have the same InfoWatch Device Monitor server application version installed compliant with the appropriate up-to-date database.

1. **Running the Installation Wizard**
Open the folder where Device Monitor distribution kit is kept. Then open the `Server` directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Setup Wizard welcome screen. Click **Next**.

2. **Accepting the License Agreement**
   Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms in the License Agreement** and click **Next.**
3. **Selecting components to install**
   Custom Setup page has all components selected by default:
   - Server
   - Management Console
   - Distribution service

   You can change the list of components you want to install. All components are to be installed on one workstation by default. If you plan to use a Management Console or Distribution service, in the opened window select **Entire feature will be unavailable**. You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location. When installing a Distribution service, a new Agents distribution kit will be automatically placed in the distribution directory.
   Click **Next**.
4. **Configuring server settings**
   On **Type of installed server** page select:
   - **Primary Server** - should be installed first. Agents and Management Console will connect to it.
   - **Secondary Server** - an additional server that balances Agents' workload.

   Warning!

   Changing the name of the Device Monitor server after installation could cause System malfunction.

   Note:

   To install a secondary server it is required first to install the primary one to a separate workstation. Secondary server installation is described in point 14.

   To ensure rapid server status updates it is recommended that you select **Publish Server in Active Directory** option.

   Warning!

   Workstations occasionally interact with the Device Monitor server to update security policies. To let the newly added server handle workstations and notify the Clients about any possible server port changes it is recommended that you publish its details in the domain during the installation.
   To publish Device Monitordataindomain, the account that installs the server needs privileges to create and delete connection points.

   If you have the Device Monitor database of the appropriate version, deselect the **Install new Database** option.
   Click **Next**.
5. **Choosing a configuration file**

If the new database installation is not performed, this step is skipped.
To use the server configuration file exported before (see "*InfoWatch Traffic Monitor. User Guide*", "Import/Export Configuration" article), click **Open** and specify the configuration file location.

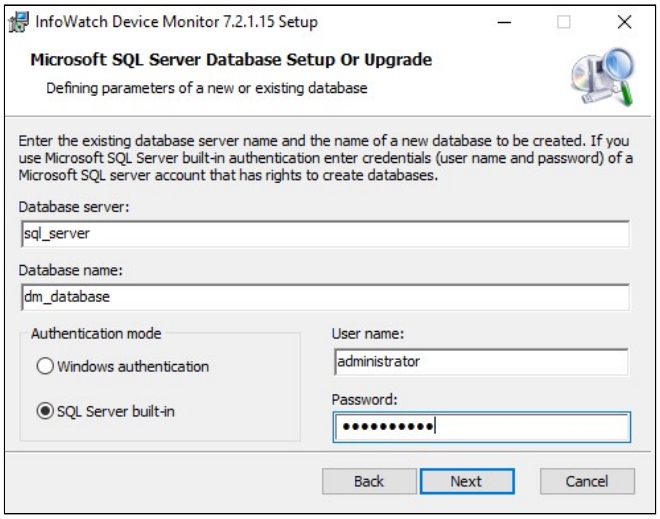
> **Warning!**
>
> The configuration file should be placed on the local hard or external device. The Setup Wizard does not support network locations.

Click **Next**. In this case, all existing settings and elements of configuration will be replaced with imported ones.

6. **Selecting database server**

   Specify DBMS that will control Device Monitor database by choosing one of the following options:
   - Microsoft SQL Server
   - Oracle
   - PostgreSQL

   If you don't want to install a new database (**Install new Database** option has not been selected in Step 4), you need to specify connectivity settings for the existing Device Monitor database.
   Click **Next**.
7. **Database configuration**
   You skip this step if you chose to use an existing database in Step 4.
   Database configuration depends on DBMS type.
   If you are using Microsoft SQL Server DBMS, specify the following parameters:
   - **Database server**. NetBIOS Microsoft SQL Server name where the database will be created. Do not enter an IP address in the **DB server** box, since this will prevent you from connecting to the database server.
     If there are any named instances on the database server, specify the server name as follows: <server_name>\<instance_name>.
   - **Database name**. New database name.
     It may contain Latin letters, numbers, and other characters except for spaces and special characters: «*», «?», «/», «\», «|», «^», «:», «"". The name must start with a Latin letter.
     The name can be 1 to 123 characters long.
   - **Authentication mode**. Database owner authentication method. For this option, specify the authentication method selected during account preparation (see "Database Deployment Managed by Microsoft SQL Server DBMS").
     If the account uses Windows authentication, select **Windows authentification**. In this case, the database will be created by the domain user, who runs the installation.
     If the account uses SQL Server authentication, select **SQL Server built-in**. Then enter username and password into **User name** and **Password** fields respectively. See the recommendations of password creation in the article "Appendix A. Username and Password Recommendations".



When using Oracle DBMS configure the following settings:

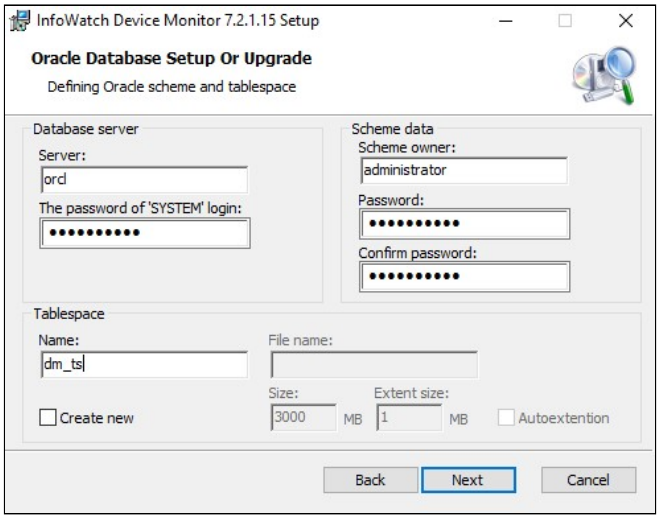
a. Set database server connection options:
- **Database server**. Database server name. For this parameter, use server alias `tns_name` from the **tnsnames.ora** file or TNS string representation.
- **The password of 'SYSTEM' login**. SYSTEM account password.

b. Specify the parameters of the database schema owner account:

> **Warning!**
>
> It is not recommended to use existing database scheme settings.

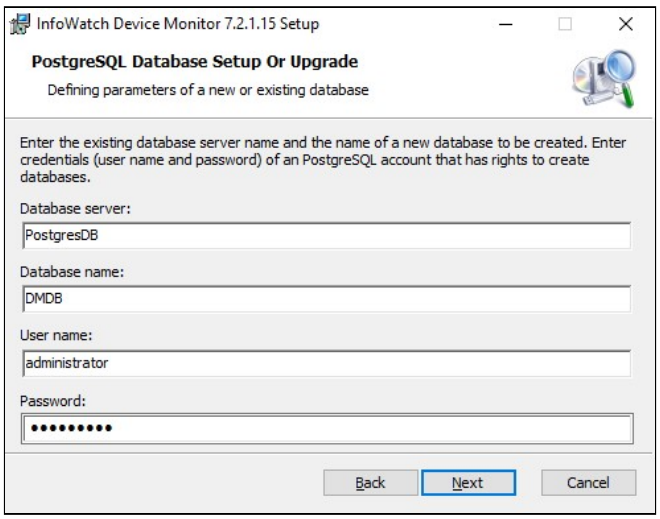
- **Scheme owner**. Database schema owner account name.
- **Password, Confirm password**. Database schema owner account password.
Password is assigned based on requirements specified in Oracle DBMS documentation.

c. Configure tablespace settings in the **Tablespace** box.
You can use an existing tablespace or create a new one. If you are using an existing tablespace, enter the tablespace name in the **Name** field.
To create a new tablespace, check the **Create new** box. Then specify tablespace options:
- **Name**. Tablespace name.
- **File name**. Name of the file where the new tablespace will be stored.
- **Size**. Maximum size (in MB) of the data file (default size is 3000 MB).
- **Extent size**. Maximum size (in MB) of a continuous segment in a data file (the default size is 1 MB).
- **Autoextension**. Automatic file extension via Oracle DBMS. If the **Autoextension** box is selected, an automatic extension is enabled (this feature is disabled by default).



When using PostgreSQL configure the following settings:

- **Database server**. The name of the PostgreSQL DBMS where the database will be created. Default port -5432. If another port is to be used, it should be specified in the format `host:port`.
- **Database name**. The name of the newly created database.
  It may contain Latin letters, numbers and other symbols excluding spaces and special symbols: «*», «?», «/», «\», «|», «^», «:», «"». The name must start with a Latin letter.
  The name can be 1 to 123 characters long.
- **User name** - the name of the account having rights for creating the DB on the PostgreSQL server.
- **Password** - the password of the account having rights for creating the DB on the PostgreSQL server.



After all necessary parameters have been configured, click **Next**.

8. **Configuring the server**

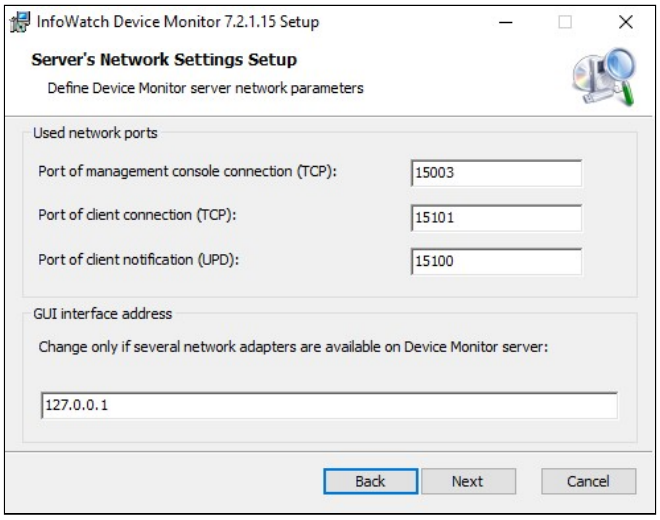
Configure Server parameters:

a. In **Used network ports** box set TCP and UDP ports used for:
   - **Management Console connection**;
   - **Clients connection** to transfer security schemes to managed workstations, send

information about events and shadow copies to the server;
- **Clients notification** about security scheme changes.

b. In **GUI interface address**, enter the IP address that will be used for interaction between Server and Management Console.

> **Warning!**
>
> This value should only be changed if the Server is installed on a computer with multiple network adapters connected to different networks. If there is one network adapter, this value must remain unchanged, otherwise, Management Console won't be able to connect to Server.
> If you add more network adapters while working with the Server, you can change this setting in the Server configuration file.



After all necessary parameters have been configured, click **Next**.

9. **Configuring secure channel**

   Specify the port used for traffic transfer between the InfoWatch Device Monitor Client and Server.
   If you install a new database (Install new Database option was selected in Step 4), then in Secure channel key area select:
   - if you perform the first installation then leave the **Create new key** setting;
   - if you used the server of version 6.0 or higher and deleted it and then you install it again, then to make Device Monitor Clients could connect and bind to the new server, you should specify the encryption key used on the old server. The recommendations on saving the encryption key are listed in "Uninstalling Device Monitor". Select **Use existing key** and specify the path to the file of the encryption key.

   Click **Next**.
   If you selected **Create new key** setting, specify the path where Device Monitor will save a file with a generated key.
10. **Configuring server account**
    Select an account used for InfoWatch Device Monitor launch according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account name and password. The name is entered in DOMAIN\USERNAME format.
    Click **Next**.
11. **Configuring server administrator account**

Provide credentials (username and password) for the server administrator account. This will be a **Super user** account (for further details, see "*InfoWatch Traffic Monitor. User Guide*", "Managing Console Accounts" section): it is used when you first connect to the server from Management Console.
Click **Next**.

12. **Configuring InfoWatch Traffic Monitor connection parameters**

    If at step 4 you decided to use an existing database (**Install New Database** option was not selected), then this step will be skipped.
    Specify InfoWatch Traffic Monitor interaction options:
    - **TM server address**. InfoWatch Traffic Monitor server address. The address must be entered in the following format:
      `host:port`
      Host parameter should contain the domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URI address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.
      Port parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 9100.

      > **Warning!**
      >
      > If you are going to integrate Device Monitor with Traffic Monitor 5.5 or earlier use format: h`ost:port,` where `port – 4101.`

    - **Number of connections**. The number of InfoWatch Traffic Monitor server connections. You can specify from 1 to 32 connections.
    - **Authorization token**. The token is used for API connection. Required for Traffic Monitor v. 6.0 or higher. Please get this token from the Traffic Monitor administrator.
    - If Device Monitor deployment scheme is not integrated with InfoWatch Traffic Monitor, select **Work in standalone mode** box. In this case, you can save captured shadow copies in the server installation directory by selecting the **Save shadow copies** box.

    Click **Next**.

13. **Completing the installation**
    Click **Install** to start Server installation.
    Follow the instructions to complete the installation.

    > **Warning!**
    >
    > Installing the server end on Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2, you will see **Windows Security** dialog window, which installs InfoWatch virtual printer, required for processing printer jobs from metro-applications. To install a virtual printer press **Install**.

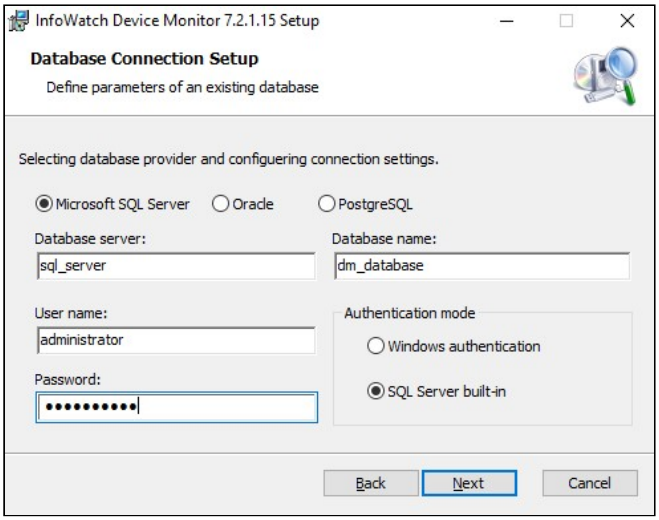
    > **Note:**
    >
    > Signature installation may take a while (up to 30 minutes).

14. **Secondary server installation**
    Secondary server activity is based on primary one, primary server settings deploy in secondary server thus guarantying Device Monitor servers connection.
    a. Running the Installation Wizard
    Open the folder where Device Monitor distribution kit is kept. Then open the `Server` directory. Run platform-specific setup file from this directory. You will be redirected to InfoWatch Device Monitor Setup Wizard welcome screen. Click **Next**.
    b. Accepting the License Agreement
    Read the End User License Agreement. If you accept the license terms, select **I accept the terms in the |License Agreement** and click **Next**.
    c. Selecting components to install
    Custom Setup page has all components selected by default:
        - Server
        - Management Console
        - Distribution service

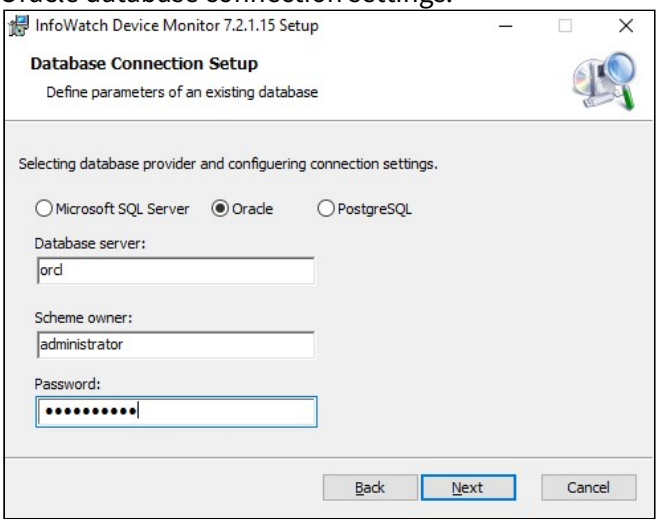
    You can change the list of components you want to install. All components are to be installed on one workstation by default. If you plan to use a Management Console or Distribution service on one workstation you do not need to install this feature:
    click **Management Console** or **Distribution service** and select **Entire feature will be unavailable** in the opened window. You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location. When installing a Distribution service, a new Agents distribution kit will be automatically placed to distribution directory.
    Click **Next**.
    d. Configuring server settings
    Select the **Secondary server** as a **Type of installed server**.

    > **Warning!**
    >
    > Secondary server installation resists new database installation, that's why it is required to specify the parameters of existing database.

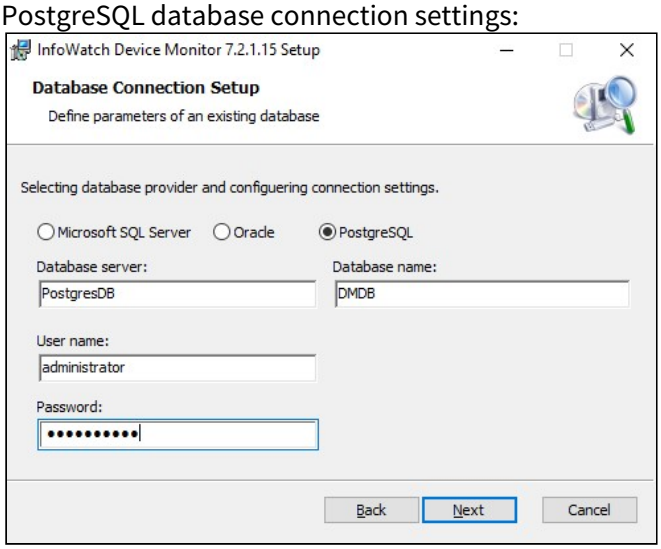
    e. Database connection setup
    Specify DBMS managing Device Monitor database and put in the rest connection parameters that were used while installing the primary server.
    Microsoft SQL Server connection settings
    If the account uses Windows authentication, and the database was created by a domain user, **Windows authentication** should be selected. If the account uses SQL server build-in authentication, select **SQL server build-in**:



Oracle database connection settings:

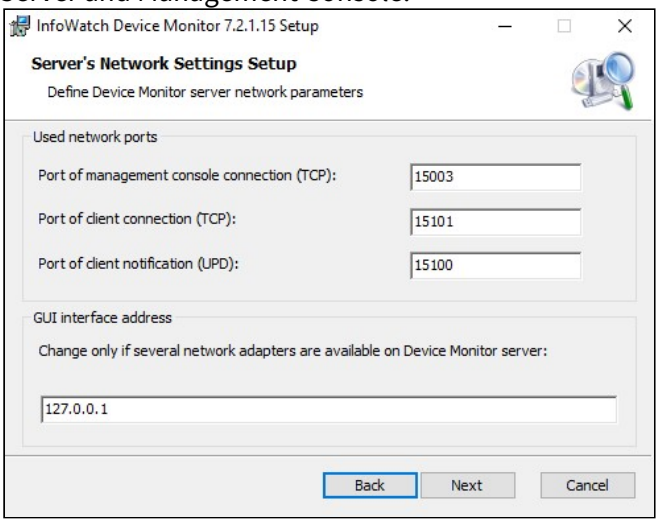


PostgreSQL database connection settings:



After all necessary parameters have been configured, click **Next**.

f. Server network parameters setup
Configure server parameters:
In **Used network ports** box set TCP and UDP ports used for:
- **Management Console connection**;
- **Agents connection** to transfer security schemes to managed workstations, send information about events and shadow copies to the server;
- **Agents notification** about security scheme changes.
In **GUI interface address**, enter an IP address that will be used for interaction between Server and Management Console.



After all necessary parameters have been configured, click **Next**.

g. Configuring server account
Select an account that will launch InfoWatch Device Monitor according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account name and password. The name is entered in DOMAIN\USERNAME format.
Click **Next**.

h. Completing the installation
Click **Install** to start server installation. Follow the instructions to complete the installation. Signature installation may take some time.

4.3 InfoWatch Device Monitor Agent Installation

Device Monitor Agent and Device Monitor server should be installed in the same time zone. This will ensure the event interception time is correct.

Warning!

InfoWatch Device Monitor Agent and InfoWatch Device Monitor server should not be installed on the same computer, otherwise this may cause the lack of server functionality.

InfoWatch Device Monitor Agent can be installed on workstations in the following ways:

- Local Installation. It uses the Setup Wizard on each computer.
- Remote installation using third-party software. It uses software distribution tools: for example, Microsoft Active Directory group policy.

- Remote installation through InfoWatch Device Monitor Management Console expansion tasks (for details, see "*Infowatch Traffic Monitor. User Guide",* "Agents Remote Installation, Updating and Uninstallation" section);
- Automatic installation through InfoWatch Device Monitor Management Console (for details, see "*Infowatch Traffic Monitor. User Guide", "Active Directory Connecting and Synchronizing*" section).

Follow the directions below to successfully install or update InfoWatch Device Monitor Agent:

1. Ensure the third-party DLP systems not to be run in parallel;
2. Include to the list of security exceptions InfoWatch Device Monitor Agent processes (the list of files you may find in "List of InfoWatch Agent's files to be added to antivirus exclusions group");
3. Disable antivirus self-protect function;
4. If possible, disable or remove the antivirus software installed when installing, updating and deleting InfoWatch Device Monitor Agent;
5. If you are using VMWare Horizon VDI 8.0.0-16530 on your workstations, then disable the component ftapihook654.dll version 3.2.4.1. (see details in the article "VmWare Horizon VDI compatibility issues")
6. Ensure the ports required for InfoWatch Device Monitor Agent proper operation are available (list of ports you may find in "*Infowatch Traffic Monitor. Administration guide*", "Configuring InfoWatch Device Monitor Server*" section*);
7. To connect, make sure the domain names of InfoWatch Device Monitor server and the computer, where InfoWatch Device Monitor Agent is to be installed are correctly resolved by DNS server into IP addresses;

   Note:

   To perform the check, run the following command within the console:

   `nslookup <hostname>`

   Example:

   `nslookup dmserv`

   If you have network problems, please contact your System Administrator.

8. If network connections settings (control panel) are not required to be used, disable it when creating InfoWatch Device Monitor Agent's distribution kit.
9. Install InfoWatch Device Monitor Agents on test workstations or on a small group of computers first;
   If there are no errors, reduced productivity, applications pending identified on test workstations during 2 or 3 days, you are advised to continue the installation on workstations.

Warning!

Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

Warning!

When you install, update or uninstall the Agent, all network connections are temporarily disconnected. This is due to the installation of network traffic control components (IWPROXY and IWNBG) that are used by Device Monitor. Besides, disconnection is related both to the technological features of the OS when installing modules and to forced restart of network cards when installing the Transparent Proxy module.

Warning!

During the Agent installation, the Mozilla Firefox, and Mozilla Thunderbird applications (if they were running) will be closed.

Note:

Before installing the Agent, it is required to run specific Windows updates for workstations on Windows 7 Service Pack 1 or Windows Server 2008 R2 OS (for details, see "Hardware and Software Requirements").

Note:

When installing the Agent on Windows 7 OS or Windows 2008 R2 Server it is recommended to consider the following point:

Corporate network control component will not be installed during the first installation of the Agent. If needed, the component can be installed manually using the command line.

Note:

Start of InfoWatch Device Monitor Agent is performed automatically after the installation. Before restarting a computer the Agent's functionality is limited only by the following issues:

- traffic interception, sent via proxy server;
- network interception (when Agent is installed on OS Windows 8 and later);
- interception of copying to external devices.

4.3.1 Standard Agent Installation

Important!

We highly recommend not installing InfoWatch Device Monitor Agents on computers with the same names. Such computers will be registered as a single computer, so the same policies will apply to them, the same events will be registered, etc.

Create an actual package to install Agent (see "Traffic Monitor. User Guide. Creating Installation Package") and write it to external device. The Agent can be installed by a user with local administrator rights on the computer.

Installing Device Monitor Agent on the computer with OS Microsoft Windows using msi package followed by manual input of parameters:

1. **Running the Installation Wizard**
   Insert the external device containing Agent's distribution kit to computer drive. Then open the `Client` directory. In the catalog find and run the package for deploying on the required platform according to the parameters specified while packages forming. For example, `InfoWatch.DeviceMonitor.Client.7.7.0.x64.msi.cmd`.
   You will be redirected to InfoWatch Device Monitor Agent Installation Wizard welcome screen.
   Click **Next** to go to the next installation screen.
2. **Choose installation directory**
   Specify the path to the Agent installation directory.

   > **Important!**
   >
   > Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the agent installation will be incorrect.

   Click **Next**.
3. **Configuring settings**

   Specify the parameters for connecting to the InfoWatch Device Monitor server:
   - **Server**. InfoWatch Device Monitor server name.
   - **Port**. Port number used for communication between InfoWatch Device Monitor Agent and Server (by default, port 15101 is specified).

   Click **Next**.

4. **Completing the installation**

   Proceed to the **Confirm installation** screen and click **Next** to start the Agent installation. Follow the instructions to complete the installation. Restart your computer, once the installation is complete.

Installing Device Monitor Agent on the computer with OS Microsoft Windows using cmd package containing installation parameters:

1. **Enter Windows command line**
   Start the command line (cmd.exe) under the Administrator account.
2. **Run the script**
   a. Go to the catalog containing the installation script:
   `cd <path_to_script>`
   b. Run the script by entering its full name, for example:
   `InfoWatch.DeviceMonitor.Client.7.7.0.x64.msi.cmd`
   c. The installation without graphic interface will start in silent mode and without notifications. Wait till the installation is compele, then the log file with detailed information will be created.

Installing Device Monitor Agent to on the computer with RED OS:

> **Note:**
>
> If your computer has a customized version of SeLinux system, we can not guarantee correct installation of Agent.

1. **Preparing fro the installation:**
   a. Copy tha archive with Device Monitor Agent installation and uninstallation package and scripts. The archive is a part of a distribution kit.
   In our example: `Setup.RedOS-7.3-iwdm.x64.7.7.0.62.tar.gz`.
   b. Go to the directory where you copied the archive and enter the unpacking command:
   `sudo tar -xvzf Setup.RedOS-7.3-iwdm.x64.7.7.0.62.tar.gz`
   As a result the following files will be created `install.sh`, `remove.sh`, `iwdm_<agent_version>.rpm`.

   > **Note:**
   >
   > When unpacking and installing Agent on OS ALT Workstation 10 use the command `su -` instead of `sudo:`
   >
   > `su - tar -xvzf Setup.AltLinux-10.0-iwdm.x64.7.7.0.84.tar.gz`

2. **Installing InfoWatch Device Monitor Agent:**
   a. Go to the directory where the content of the archive **`Setup.RedOS-7.3-iwdm.x64.7.7.0.62.tar.gz`** is unpacked.
   b. To install the Agent you need to run script by entering the command:
   `sudo ./install.sh <server>:<port>`
   `where <server>` - ip-address or domain name of Infowatch Device Monitor server,
   `<port>` - port to connect to Infowatch Device Monitor server.
   In our example the command is:
   `sudo ./install.sh <dm-server>:<15101>`
   The product will be installed in the directory `/opt/iw/dmagent`.
   c. You can check the status of services by entering the following command:
   `sudo systemctl status iwdm*`

4.3.2 Agent Installation via Software Distribution Tools

The corporate network administrator can perform Client centralized setup via software distribution tools. This section describes installation from Microsoft Active Directory.

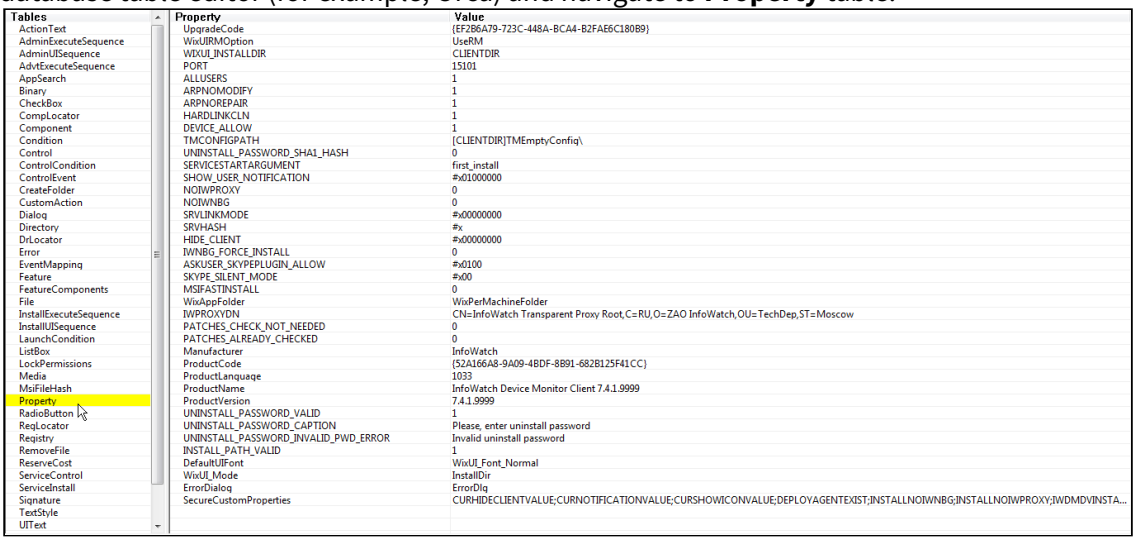
Agent installation from Microsoft Active Directory is carried out via group policy. To do so, you have to select a group policy that covers all target workstations. This policy may be assigned to:

- Active Directory container that holds all target workstations
- the whole Active Directory domain, but not default domain policy. This policy should only cover the group that includes all controlled workstations.

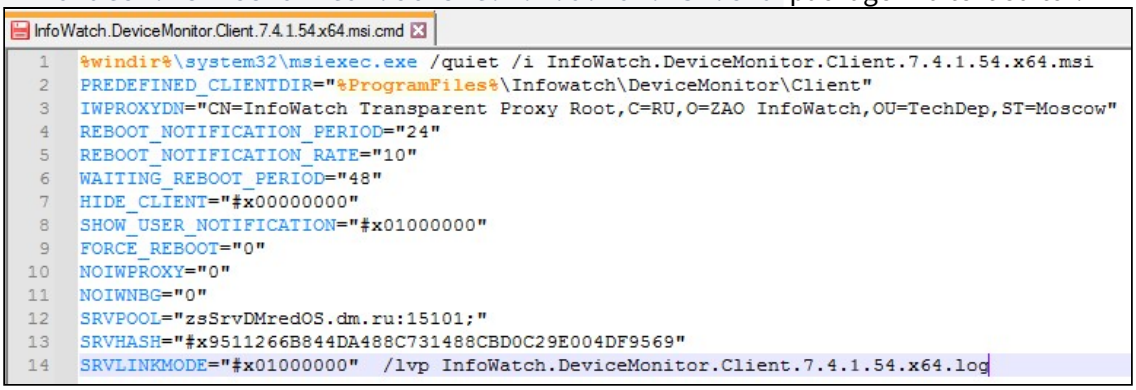
1. **Creating Installation Package**

a. Create `cmd` installation package, for example, `InfoWatch.DeviceMonitor.Client.7.7.0.x64.msi.cmd` as described in "*Infowatch Device Monitor. User Guide*", "Creating Installation Package" article).
b. Put the installation package to the network directory that can be read by all target computers within the domain.

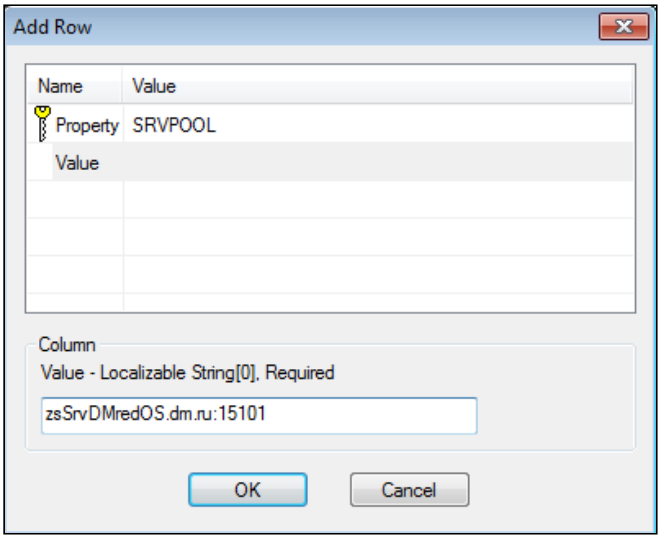
2. **Creating Transform File**
   a. Open the `InfoWatch.DeviceMonitor.Client.7.7.0.x64.msi` installation file in a database table editor (for example, Orca) and navigate to **Property** table:



   b. In the menu bar, select **Transform** → **New Transform**
   c. Open the previously created `InfoWatch.DeviceMonitor.Client.7.7.0.x64.msi.cmd` package in a text editor:



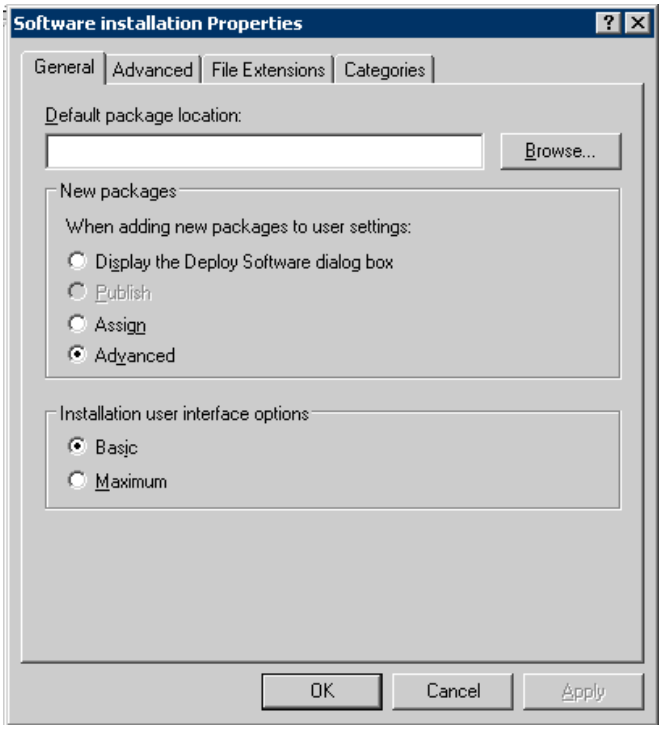
   d. In the **Property** table, add missing properties or replace old property values with the new ones from the `cmd` package. To add a new property:
      i. Click on an empty row in the table.
      ii. Enter name-value pairs in the format <property name>=<"new value"> and click **OK**. Use ";" as a separator to enter several values.



iii. To replace a property value, double-click the property value, enter the new value and press **Enter**.
Perform the steps above for all properties from the `cmd` package.

e. In the menu bar, select **Transform** → **Generate Transform**
f. Save the `mst` transform file.

3. **Editing Group Policy**
Edit group policy before installing Agent from Active Directory.
To edit group policy:
   a. Open **Active directory users and computers** (**Start** > **Settings** > **Control Panel** > **Administrative tools** > **Active directory users and computers**).
   b. In the console tree, select Active Directory container with all target workstations.
   c. Open **Group Policy**. To do this, click **Properties** in Active Directory container context menu. In the following dialog box, navigate to **Group policy** tab. On this tab, select group policy and click **Edit**.
   d. In the console tree, select **Software Installation** (**Computer Configuration** > **Software Settings**).
   e. In **Software Installation** context menu, select **Properties**. On General tab configure the following settings (see the picture below):
   - set **New packages** value to **Advanced**;
   - set **Installation user interface options** value to **Basic**.



f. When the configuration is complete, click **OK**.

4. **Preparing Agent installation task**

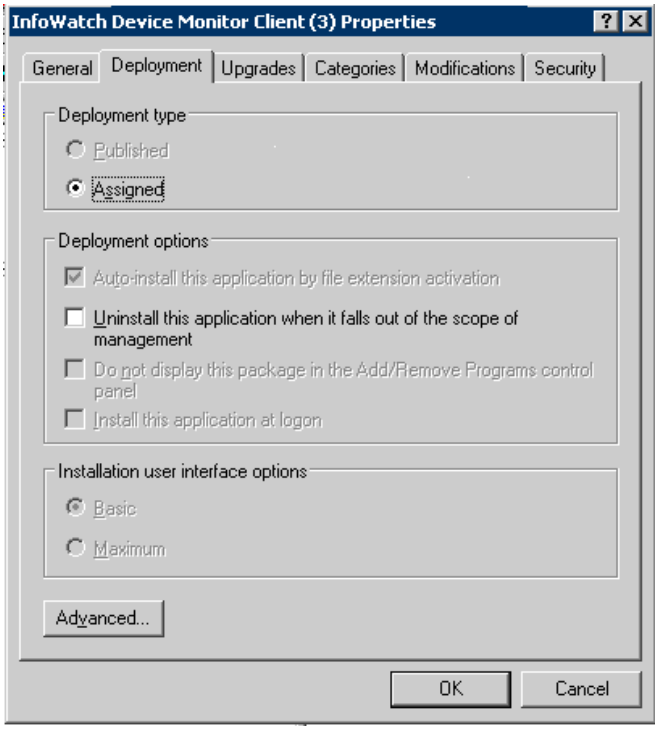
Agent installation task is created and configured on **Group Policy Object Editor** screen:

a. After opening **Group Policy Object Editor** box select **Software Settings** (**Computer Configuration** > **Software Settings**) in the console tree. Right-click the selected item and then select **New** > **Package**.

b. In the following **Open** dialog specify the `mst` transform file (first move the `msi` installation package to a network directory that is readable for all installation-target computers within the domain).

> **Note:**
>
> Some distribution systems allow you to specify deployment options. In such cases, you can pass the `InfoWatch.DeviceMonitor.Client.7.7.0.x64.msi.cmd` package directly to the distribution system.

c. Configure new package properties:
- Make sure all settings in **Deployment** tab comply with the following figure.



- After all necessary settings have been configured, click **OK**.

d. In the console tree, select **Computer Configuration** > **Administrative templates** > **System** > **Scripts**. In details section, select **Run logon scripts synchronously**. Then set the value to **Enabled** in properties screen.

5. **Setup**

New task appears in **Software Installation** task list. The task is carried out as soon as the target computer is restarted. InfoWatch Device Monitor Agent starts automatically after its installation. Installation method is displayed in **Deployment state** column. **Assigned** status means that installation is forced, i.e. doesn't need an approval of target computer user. **Published** state means installation upon user's approval.

> **Important!**
>
> You can check if the Agent has been installed successfully in InfoWatch Device Monitor Management Console. All workstations the Agent has been successfully installed to must appear in the list in **Workstations** area. To view all managed workstations, click **Show all workstations** at the top of Navigation Pane. To obtain up-to-date Agent information, click **Update** in Toolbar.

5 Configuring InfoWatch Device Monitor Server

This section contains describes low-level configuration of InfoWatch Device Monitor Server. We recommend performing actions described only with the help of InfoWatch technical support engineers.

To ensure the correct operation of InfoWatch Device Monitor, make sure that the following ports are open on the computers, where Device Monitor components are installed:

Default port	Supported protocols	InfoWatch Device Monitor computers		Description
		Source	Receiver	
15003	TCP	Management console	Server	Connecting InfoWatch Device Monitor console to server
15004	TCP	Agent	Server	Encrypted connections to InfoWatch Device Monitor Agents
15100	UDP	Server	Agent	Notifying InfoWatch Device Monitor Agents (for example, if the security scheme or the server configuration has been changed)
15101	TCP	Agent	Server	Notifying InfoWatch Device Monitor Agents about server capability
15505	TCP	Server	Agent	Distribution, update and removal of InfoWatch Device Monitor Agents
15506	TCP	Server	Agent	Collecting logs, enabling/disabling the debug mode
local port, dynamically generated	TCP	Agent		The Agent module in a user session, the `DM.Client.exe` process
15200	TCP	Server	Distribution Agent	Downloading InfoWatch Device Monitor Agent distribution kit

The server is configured by means of `InfoWatch.DeviceMonitor.Server.exe.config` XML configuration file. The configuration file is located in the same directory as the `InfoWatch.DeviceMonitor.Server.exe` server executable file.

By default, after its installation, the Server is located in the following directory:

`C:\Program Files\InfoWatch\Device Monitor\Server`.

You can view the configuration file using any text or XML editor. The file encoding is UTF-8.

The root element of the configuration file is the `<configuration>` element. The root element includes child elements (configuration sections). The table below contains the configuration file structure and a description of its sections. Links in section names provide detailed information on the section configuration.

Important!

We highly recommend editing the configuration file only with the help of InfoWatch technical support engineers.

When you finish editing, restart the Device Monitor Server.

Configuration section	Description
<configSections>	Service section. Contains a description of all other sections. Editing this section is not allowed.
<runtime>	Contains settings for the Microsoft .NET Framework runtime. These settings are required for the correct operation of the Server. The `<runtime>` section defines the `gcServer` element for configuring the garbage collector. The element has the `enabled` attribute that takes the value `true` (parallel garbage collection is enabled) or `false` (parallel garbage collection is disabled). We recommend not editing this section.
<applicationSettings>	Contains settings for individual Server modules, such as ports, buffer sizes, timeouts, etc.
<system diagnostics>	Contains logging settings. Logging can be useful for diagnosing the operation of the Server components.

If you need to delete temporary files generated by Device Monitor, you can do it using a special utility: for details, see "Deleting Device Monitor Temporary Files".

5.1 <applicationSettings> Section

You can use <applicationSettings> section to configure individual Server modules. There are six modules. All sections have the same structure: Each section includes a set of elements for module configuration. Each <setting> element has the following attributes:

- `name` - setting name.
- `serializeAs` - data serialization method. Data is always serialized as a string (string data type).

Module parameters are defined by <value> child element. For example:

```
<setting name="RemotingPort" serializeAs="String">
<value>15003</value>
</setting>
```

Each module parameters are described in the following table.

Section of configuration file	Description
<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings> Server kernel configuration	
RemotingPort	TCP port processing Management Console service connections. Default value `15003` (it is not recommended to change this value)
CultureName	Language of module diagnostic and other messages. Possible values: • `ru-RU` • `en-US`
MachineName	IP address of network interface used by the Server to accept Management Console connections. Default value `127.0.0.1` . You can only change this value if the Server has 2 or more network interfaces. In this case, you should explicitly specify interface address used by the Server to accept incoming connections from different instances of the Management Console
CheckServerSettingsInterval	If clustering is enabled – a period of synchronization with the database (in seconds). When the specified period expires, the Server queries the database for changes in the security scheme made by the main Server that uses the same database. Default value `300`
<InfoWatch.DeviceMonitor.Server.Database.Propert	
DatabaseType	Database types. Possible values: • `Oracle` • `Microsoft` • `PostgreSql`

Section of configuration file	Description
ConnectionString	Database connection string. It must comply with ADO.NET connection string rules. For example: Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=True
CultureName	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
ConnectionPoolSize	The number of open connections to the database that will be used by the server. Default value `200`
CommunicationPort	The port number that is used when the server connects to the Deployment Agent if the Agent is installed through installation tasks. We recommend not changing this value during the System operation. Default value `15505`
UpdateStatusTimeOut	The interval of updating the job execution state on a remote computer. The server gets the installation state on the computers where the Agent is deployed and displays this state. Default value `60`
EventRelationStoredPeriod	The interval in days. The parameter is used in formula to calculate the date of removal when cleaning up garbage events. Default value `7`
DeleteEventCount	Maximum number of events to be deleted from the DB at a time. Default value `10000`
`<InfoWatch DeviceMonitor.Server.Gui.Properties.Settings>` Management Console interface module settings	

Section of configuration file	Description
CultureName	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
InitialLeaseTime	Time (in minutes) during which a connection session with the Management Console is valid Default value `5`
RenewOnCallTime	Time (in minutes) for which a connection session with the Management Console is prolonged Default value `2`
<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings> Settings of the module that serves client connections (controlled computers)	
Backlog	Queue length of client connections waiting to be connected. Default value `64`
CultureName	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
ShadowCopyTempDir	A full path to the directory which stores temporary shadow copies waiting to be sent to InfoWatch Traffic Monitor. The default value: `C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir\<0÷255>\`
DmpV1Address	List of IP addresses (separated by ";") on which the server listens to ports. Possible values: • `AllAny` – ports on all IP addresses of the computer (the default value)

Section of configuration file	Description
	• `AllIp4` – ports on all IP addresses of version 4 • `AllIp6` – ports on all IP addresses of version 6
Dmpv1TraceLevel	Trace level of interaction protocol between client and server. Possible values: • 1 – disable tracing • 2 – only trace information on packages (the default value) • 3 – full tracing Tracing is output to the receiver of diagnostic messages (Windows Application Log by default) only of the value is `3` and logging level for the module filter is `Verbose` (see "<system.diagnostics> Section").
Dmpv1TraceClients	List of Agent IP addresses (separated by ";") that require tracing. If the value is `All`, then all Agents are traced.
Dmpv1ConnectionsLimit	Number of simultaneously processed TCP/IP connections with Agents. Default value `400`
Dmpv1ConnectionsQueueLimit	The maximum number of connections waiting for processing. If the number is exceeded, connections are reduced to the value of Dmpv1ConnectionsQueueLengthAfterCut parameter. Default value `700`
Dmpv1ConnectionsQueueLengthAfterCut	The number of connections after reducing the queue which exceeded the maximum size. Default value `250`
TimeoutPeriodSeconds	Timeout after which a hanging connection between Agent and Server is terminated and partially created shadow copies are deleted (shadow copies will be re-sent when a new

Section of configuration file	Description
	connection is established). Default value `120`
SSLPort	The port number for encrypted connections. Default value `15004`
CheckUpdateTmConfigPeriodMinutes	TM server query period (in minutes) checking for configuration changes. Default value `30`
`<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>` Basic settings for Traffic Monitor Server connector	
DBPollTime	Database query period (in milliseconds) checking for database events Default value - `10 000` Minimum value - `1000`, maximum value - `600000`
CultureName	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
NumberOfConnections	Number of connections to InfoWatch Traffic Monitor. Default value - `4`. Minimum value - `1`, maximum value `32`.
MaxSendEventCount	The maximum number of events that is being read from DB at a time, to be sent to TM Default value `1000` Minimum value - `1`, maximum value `10000`.
ShadowCopyTrasferBlockSize	The size of a shadow copy data block sent to Traffic Monitor server, in MB. Default value `16` Minimum value - `1`, maximum value - `64`.

Section of configuration file	Description
`<InfoWatch DeviceMonitor Database.Core.Properties.Settings>` Settings of database low-level driver	
CultureName	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`
MaxConnectionWaitingTime	Waiting time for a free connection from the pool, in seconds. Default value `300`
CommandTimeoutSeconds	Execution time of a long operation or a queue, in seconds. Default value `30` **Note:** This setting does not apply in Oracle DBMS.
LongCommandTimeoutSeconds	Execution time of a long operation or a queue, in seconds. Applies when the execution time is a significant interval. Default value `300` (0 endless). **Note:** This setting does not apply in Oracle DBMS.
`<InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings>` Settings of the module that interacts with Platform	
EPAddress	Address of the Platform server and Platform token. The System does not use the values of these parameters.
EPToken	

Section of configuration file	Description
DBPollTime	Frequency of the database poll (in ms). Default value - `5000` Minimum value - `5000`, maximum value - `600000`
CultureName	Language of diagnostic and other messages of the module. Possible values: • `ru-RU` • `en-US`
NumberOfConnections	The number of connections of the IW Device Monitor server to the Platform server. Default value `4` Minimum value - `1`, maximum value - `64`
MaxSendEventCount	The number of events that can be sent from the database at a time. Default value `5000` Minimum value - `1`, maximum value - `10000`
RequestEventCount	The number of statistics events that can be sent as one batch. Default value `100` Minimum value - `1`, maximum value - `10000`
WriteDisconnectEventLogInvervalMinute	Log file recording interval if the connection is broken or interrupted (in minutes). Default value `60` Minimum value - `10`, maximum value - `240`
WaitPlatformDiskErrInitialMinute	Initial number of minutes to wait in case of error 507 before retrying to send events to Platform. Default value: `10` Minimum value - `1`, maximum value - `1440`
WaitPlatformDiskErrMaxMinute	Maximum number of minutes to wait in case of error 507 before retrying to send events to Platform.

Section of configuration file	Description
	Default value: `60` Minimum value - `1`, maximum value - `1440`
`<InfoWatch.DeploymentSubSystem.Properties.Settings>` Settings of the module that distributes (installation/update/removal) Agents and diagnostics	
NetworkLatency	Technical parameter, not recommended to change.
RunningInstallationsLimit	The maximum number of primary simultaneous installations on computers Default value `0` (calculated according to formula)
BandwidthUsagePercentLimit	Controllable percent of network capacity the tasks can take Default value if no error or parameter specified `0.5` (`50%`)

5.2 <system.diagnostics> Section

Server diagnostics section. It includes the following elements:

- `<trace>`. Diagnostics module general settings.
- `<sources>`. Individual Server components diagnostics settings.
- `<switches>`. Managing diagnostic system's overall level of detail. Includes detalizer definitions. Typically, there is a single detilizer. If different modules require different detalisation settings, you should use a filter. General detalizer's value must contain maximum detail.

<*trace*> element

Used to describe global module diagnostics settings. In this element you can specify message margins and diagnostics data saving parameters.

<*sources*> element

Used to configure individual application modules. Includes <source> child elements - one for each application module (see Server module list in "<applicationSettings> section").

The list of modules also includes secondary ones which are needed for debugging output for main components:

- `InfoWatch.DeviceMonitor.Server.FileIdentification.Core` - module describing the signatures object model;
- `InfoWatch.DeploymentSubSystem` - module of the subsystem responsible for deployment on computers;
- `InfoWatch.DeviceMonitor.EventPostProcessorManager` - module for post-processing of print events;

- `InfoWatch.DeviceMonitor.ScreenShotStorage` - module for saving screenshots on the file system;
- `InfoWatch.DeviceMonitor.Server.Remote.Install` - module for launching the remote installation\update\uninstallation of the Agent on the computer.

`<source>` element has the following attributes:

- `name`. Server module name.
- `switchName`. Name of the module that defines diagnostics (detalizer's) level of detail.
- `switchType`. Type of the module that defines diagnosis level of detail. Is always set to `System.Diagnostics.SourceSwitch`.

Each `<source>` element also contains a definition for diagnostic messages receiver (`<listeners>`). Diagnostic messages can be received by:

- Windows application log (Application log);
- system debug output (can be viewed with special tools like DebugView);
- text file.

`<source>` element has child element `<listeners>`. This element contains parameters of diagnostic messages receiver. `<listeners>` element may contain the following child elements:

- <add>. Add a new diagnostic messages receiver
- <remove>. Deleting diagnostic messages receiver. You can only apply it to remove default message receiver (Windows application log). To this end, set element name to `Default`: `<remove name="Default" />`

<*add*> element

This item adds diagnostic messages receiver to Server module. Element contains the following attributes:

- `name`. Diagnostic messages receiver name.
- `type`. Diagnostic messages receiver type.
- `initializeData`. Server module ID. Typically, this value is the same as Server module name. If Windows application log is the receiver, this information appears in the source column.

Receiver type is fully qualified receiver name from .NET framework library or proprietary type that implements the required diagnostic messages receiver interface.

.NET framework library contains the following diagnostic messages receiver types:

- `System.Diagnostics.EventLogTraceListener`. Windows application log
- `System.Diagnostics.ConsoleTraceListener`. Console application message output
- `System.Diagnostics.TextWriterTraceListener`. Text file output
- `System.Diagnostics.DefaultTraceListener`. Debug Windows output (enabled by default).

<add> element also contains diagnostic messages filter. This filter only displays the messages with level of detail exceeding the filter parameters. It features the following levels of detail (listed in descending priority order):

- `Verbose`. Debug level. All events are logged. This level can only be used for System debugging. This level does not allowed for a system running in normal mode, since it cuts the performance significantly.
- `Information`. Information level. Registers the events that are not related to errors, for example, information on server changes.
- `Warning`. Warning level. Registers non-critical System errors, such as an unexpected disconnection from the Server, connection timeout, etc.
- `Error`. Error level. Records errors that cause System malfunction (i.e., errors that require troubleshooting).
- `Critical`. Critical level. Registers serious malfunctions that can lead to System shutdown.

Example 1

Detalizer features *Verbose* logging level, while module filters feature *Warning* level. Then detalizer ignores *Warning*, *Error* and *Critical* events, but filters out *Information* and *Verbose* events.

Example 2

Detalizer features *Error* logging level, while module filters feature *Warning* level. In this case, detalizer ignores *Error* and *Critical* events, but filters out *Warning*, *Information* and *Verbose* events. This happens because overall System level of detail is *Error*, i.e. only *Error* events and higher are registered regardless the filter settings.

<*remove*> element

Deleting message receiver. It is usually used to remove default receiver that displays diagnostic messages in Windows debug output:

```
<remove name="Default" />
```

<*switches*> element

Defines Server detalizers. Typically, there is only one detalizer, which sets the global (for entire Server) level of detail the diagnostic system. If individual Server modules require lower level of detail, you can use filters.

`<switches>` element contains only one child element by default:

```
<add name="eventLog" value="Warning"/>
```

Level of detail is specified as `value` attribute.

5.3 Deleting Device Monitor temporary files

InfoWatch Device Monitor provides a means for deleting the files generated by the System, namely:

- all files from the temporary files directory of the operating system (%Temp%);
- data from file queue of Device Monitor events processing (`C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir` by default; see information on the path configuring in "Раздел <applicationSettings>").

The deleting is performed by `RemShadowCopyFiles` utility located in the Server installation folder (`C:\Program Files\InfoWatch\DeviceMonitor\Server` by default).

The launching of the utility should be performed by administrator account having rights for reading and writing in directories containing deleting files.

Important!

The System will stop the proceeding of incoming events for a time when deleting procedure runs.

The procedure will delete all the data on events which were not proceeded by the moment of deleting start.

To delete temporary files:

1. Log on at the InfoWatch Device Monitor Server where you need to delete temporary files.
2. Run `RemShadowCopyFiles` utility.
3. Confirm deletion by pressing **Y**.

The utility will stop all Device Monitor services, delete temporary files and start Device Monitor services again.

Important!

When deleting temporary files from %Temp% system folder the access denial can arise: there can be some files created and used by another processes irrelevant to the System.

5.4 Configuring protection against guessing for Device Monitor

To protect the System, the following feature is enabled: in the case of repeated unsuccessful authorization attempts, user login is blocked. Protection against password guessing is configured in the database. By default, the protection is disabled.

To enable protection for Device Monitor server:

1. Connect directly to the database, which is used by the Device Monitor server.
2. Find the `PasswordProtection` table.
3. Find the following three parameters that are responsible for setting up protection:
   - **`MaxAuthFailCount`** – the number of unsuccessful login attempts allowed;
   - **`MaxBlockingTimeInSeconds`** – the time for which the login is blocked, in seconds;
   - **`MaxFailAuthPeriodInSeconds`** – the period of unsuccessful login attempts, in seconds.
4. Set the values for all three parameters in accordance with security requirements.

   Important!

   If any parameter has an incorrect value or its value is 0, protection will be disabled.

5. To apply the settings, save changes in the database.

   Important!

   Protection against password guessing will work only for Device Monitor users. When assigning rights to log into Device Monitor for AD domain accounts, you should configure protection using the AD tools.
   When restarting the DM service, the login attempt is considered to be the first one. If the user has made 3 unsuccessful login attempts in a row, then the fourth attempt after restart will be considered the first one.

If login is blocked, a new event is created in the audit log (the **Log** button in the Navigation pane) where the unlocking time is specified. When the blocked user tries to log into the System again, he/she will be notified that the number of failed login attempts has been exceeded.

An **example** of protection settings for both components:

- `MaxAuthFailCount – 5`
- `MaxBlockingTimeInSeconds – 300`
- `MaxFailAuthPeriodInSeconds – 120`

How these settings work: if during 2 minutes (120 seconds), the user makes 5 unsuccessful login attempts, then login for this user is blocked for 5 minutes (300 seconds). The countdown period of unsuccessful attempts starts from the first attempt. If during 120 seconds the user makes only 4 unsuccessful login attempts, then the next attempt will relate to a new period.

6 Updating InfoWatch Device Monitor

If you have InfoWatch Device Monitor installed, you can update it to a later version.

> **Warning!**
>
> To ensure the correct operation and all the functionalities available Traffic Monitor and Device Monitor versions should comply. See more details about Device Monitor compatibility in the InfoWatchKnowledge Base article "Compatibility among the versions of TM, DM and Agents".

The System update is similar to its installation:

1. Updating InfoWatch Device Monitor Server End (database, server, and Management Console).

   > **Warning!**
   >
   > When updating the System from early versions:
   >
   > 1. Follow the procedure: Device Monitor server should be updated first, then update Traffic Monitor Server and after this DM Agents should be updated on workstations.
   > 2. If you want to update System version 3.4 - 4.0, delete the old server version (don't remove the database) and re-install the server, configuring the connection to an existing database.
   > 3. If you want to update Device Monitor starting from version 4.0, use the standard procedure.
   > 4. When updating Device Monitor version 6.0 by deleting and then installing the Server, you must perform the following actions to let Device Monitor Agents connect to the new Server:
   >
   > - When deleting - save encryption key stored in the DM Server installation folder, `SSLServerKey.pfx` file.
   >
   > - When installing - specify the path to the saved encryption key used on the old Server.

2. Updating InfoWatch Device Monitor Agent.

   > **Warning!**
   >
   > Device Monitor Agents should be updated after the Device Monitor Server and Traffic Monitor Server have been updated.

6.1 Updating InfoWatch Device Monitor Server End

> **Important!**
>
> When several servers are used, the main server shall be updated first. All the secondary servers shall be turned off at the same time. All the servers are to be updated in turn after the main one.

Step 1. Start update

Open the folder where Device Monitor distribution kit is kept. Then open the Server directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Installation Wizard welcome screen. Click **Next** to go to the next installation screen.

Step 2. Accepting the License Agreement

Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms** in **the License Agreement** and click **Next**.

Step 3. Database configuration

The database is preserved during the update, and **Configure Database Connection** box automatically displays old database parameters. However, depending on DBMS, you need to specify particular settings.

Built-in Database Update

Skip this step if you are using a built-in DB.

Update Database Under Microsoft SQL Server DBMS

On the **Authentication Method** panel, select the authentication method for the user, who updates the database. For this option, specify the authentication method selected during account preparation (see "Database deployment under Microsoft SQL Server DBMS").

If the account uses Windows authentication, select **Windows authentication**.

If the account uses built-in SQL Server authentication, select **SQL Server built-in**. Then enter login and password into **User name** and **Password** fields respectively.

> **Note:**
>
> You can specify old or new authentication parameters as the update proceeds. For guidelines on authentication methods and account preparation see the section "Database deployment under Microsoft SQL Server DBMS".

Update Database Under Oracle DBMS

On the **DB Server** panel, specify **Password for 'SYSTEM'** - password for SYSTEM account that manages the database, which is being updated.

On the **Scheme Information** panel, fill in **Password**, **Confirm password** fields - password for database scheme owner's account used for database update.

Update PostgreSQL Database

Enter the password of the account that manages the updated database into the **Password** field.

After you have configured all parameters, click **Next**.

Step 4. update Completion

Go to the next screen and click **Install** to run System server update.

Follow Setup Wizard's instructions to complete System server update.

> **Note:**
>
> While updating Device Monitor server the filters conversion cannot be supported.

Important!

If after updating the Device Monitor Server, the `InfoWatch.DeviceMonitor.Server.exe.config` configuration file does not contain parameters for integration with InfoWatch Activity Monitor, take steps described in the KB article.

Note:

After updating the server, the **Status** field of Agent can have one of the following values:

- **Not specified** - if Agent had no connection to the server;
- **Specified** - if Agent established at least one connection to the server.

The actual status of the **Agent Activity** field is set according to the values specified in settings.

When updating to a new version, workstations that already are in the security scheme, are not renamed. A new checking and registration procedure will apply only to computers that will address the server after the update. This procedure checks only the identifier: if it matches, the workstation is renamed, and its old name is only displayed in the DM Management console until the user deletes it

The procedure that was used before checked also the name, which was the reason why the DM Management console could have two records for the same workstation, with its new and old name.

6.2 Updating InfoWatch Device Monitor Agent

Device Monitor is compatible with Agent version 7.2 and later. Therefore, updated Device Monitor components can work with older versions of the Agent. However, you can update it to a later version.

To update InfoWatch Device Monitor Agent successfully, follow the instructions at the InfoWatch Device Monitor Agent Installation page. You can use one of the following ways to update Device Monitor:

- automatic update;
- centralized update via the Management Console;
- remote update using software distribution tools;
- local update using the installation wizard;
- local update of Agents on computers running Linux using a script (as described below).

To update Agents locally on computers running Linux:

1. Follow step 1 of the instruction for the local installation (see "InfoWatch Device Monitor Agent Installation").
2. Open the directory where you have unpacked the archive.
3. Run the update script using the following command:
   `sudo ./upgrade.sh`
4. Wait for the update to finish. You can check the execution status by running the command:
   `sudo systemctl status iwdm*`

When updating Device Monitor Agent to a new version, take the following steps:

1. Update agent on a group up to 10 computers. Make sure that there are no performance errors for 2-3 days.
2. Update agent on a group up to 50 computers. Make sure that there are no performance errors for 2-3 days.

3. Update agent on a group up to 500 computers. Make sure that there are no performance errors for 2-3 days.
4. Update agent on a group up to 1000 computers. Make sure that there are no performance errors for 2-3 days.
5. Complete the update procedure with the rest of the computers.

Note:

When updating the Agent on Windows 7 OS or Windows 2008 R2 Server, note that:

If the **Corporate network control** component was installed before, it will be removed during the update. If necessary, you can install the component manually from the command line.

Warning!

After the update, reboot the workstation, so that applications started before the update could use the new interception mechanism.

7 Uninstalling Device Monitor

Important!

If you are planning to install Device Monitor Server again, then to make Device Monitor Agents could connect and bind to the new server, then starting from version 6.0 you must save the encryption key of the old server.

The encryption key is stored in the installation folder of the InfoWatch Device Monitor Server, `SSLServerKey.pfx` file.

To remove InfoWatch Device Monitor server end with Management Console and Distribution service:

1. Take one of the following steps:
   - Open `Setup\Unified` catalogue on the Installation CD. Run platform-specific setup file from this directory.
   - Run **Uninstall or remove programs** from Windows Control Panel, select **InfoWatch Device Monitor** and click **Change**.
2. On **Change, repair or remove…** screen select **Remove**.
3. To remove the system and its database, flag **Remove database** on **Remove database…** screen. Then specify parameters for uninstalling: parameters depend on your DBMS:
   - **Microsoft SQL Server** – specify your authentication method by selecting it in Authentication Method pane (see "Database Deployment Managed by Microsoft SQL Server DBMS").
     In case of SQL-server based authentication (**Integrated into SQL Server**) enter the credentials you used to connect to the database in **Login** and **Password** boxes of **Database Administrator** pane.
   - **Oracle** – enter the password into **The password of 'SYSTEM' login** box. This will remove database schema owner account and all its objects except the tablespace.
   - **PostgreSQL** –enter the credentials used to create the DB during server setup into User name and Password boxes (see "InfoWatch Device Monitor Server End Installation Procedure").

   Important!

   If the database is not working or working partially, then to delete the InfoWatch Device Monitor you should uncheck the **Remove database** field, otherwise, the deletion can be performed incompletely.

4. After specifying the parameters click **Next** and then click **Remove** to start uninstallation.

To remove only InfoWatch Device Monitor server end or Management Console or Distribution service:

1. Run **Add or remove programs** and click **Change**.
2. In **Custom Setup** click  to the left of the elements you want to remove and select **Disable this element**. Click **Next**.
3. If you selected server uninstallation at the previous step, specify whether you want to remove the database and enter the authorized account parameters, if necessary, on **Remove database…** screen (see details above).
4. Click **Change** to start uninstallation.

Warning!

When Distribution service is removed the distribution point and directory containing ditribution kits are to be removed as well.

To remove InfoWatch Device Monitor Agent:

run **Add or remove programs**, select **InfoWatch Device Monitor Agent** and click **Remove**.

You can also use centralized uninstallation to remove Agents:

- with Active Directory tools (if Agents were installed via software distribution tools) as described in "Remove Agent installed via Software Distribution Tools".
- with Management Console distribution tasks (for details, see "*InfoWatch Traffic Monitor. Administration Guide*", "Agents Remote Setup, Updating and Uninstallation" section).

Important!

Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

If you encounter any difficulties removing Agent, please contact our technical support at support@infowatch.com.

You can also visit the technical support section on our website: http://www.infowatch.com/support.

7.1 Remove Agent Installed via Software Distribution Tools

If the agent was installed via software distribution tools, you can use them to remove it.

For example, if Agents were installed via Microsoft Active Directory, the corporate network administrator can use group policy to remove the installation task. Group policy editing procedure is described in "Agent Installation via Software Distribution Tools", step 3.

To remove Agent from all managed workstations:

1. Select the installation task you want to remove. Then right-click the selected row and select **All tasks** > **Remove**.
2. Select **Remove software** in **Immediately uninstall software from users and computers** dialog.

   Note:

   Other options remove installation task without uninstalling all existing Agents. After that, you won't be able to remove these Agents with Microsoft Active Directory tools.

3. Click **OK**. The Agent will be removed from all computers under selected group policy.

To remove InfoWatch Device Monitor Agent which was installed to OS Astra Linux, please run the following command:

dpkg --purge iwdm

8 Appendix A. Username and Password Recommendations

Requirements for usernames

- The username should be 1-20 characters long.
- The username may include English letters, digits, and underscore "_". It must begin with a letter.

Requirements for passwords

- The user password should be 8-128 characters long.
- The user password may cinclude the characters in accordance with any three conditions from the follwing four:

1. Capital letters in Latin characters (A-Z)
2. Lowercase letters in Latin characters (a-z)
3. Arabic numerals (0-9)
4. Characters: «#», «$», «!» or «%»

- The user password should not contain username or a part of username.
- The password is case-sensitive.

Requirements for DB user's passwords

- The user password should not contain the symbols «"» and «'».

Recommendations for strong passwords

- Recommended password length is 10-30 characters.
- The password must contain letters, digits, and characters.
- It is not advised to:
    - Include whole words or phrases into a password.
    - Use a series of the same character.
    - Start and end the password with the same character.
    - Create a new password by adding characters to your current password.

General recommendations

It is not recommended beginning a username or password with combinations: SYS_ and ORA_.
It is not recommended using Oracle reserved words in usernames or passwords:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE
AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT
AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL

AUDITBETWEEN	HAVING	OF	SYNONYM
BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE
CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH