InfoWatch Device Monitor. Installation, Configuration and Administration Guide

06/07/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 5

2 Set of Documents 6

3 Hardware and Software Requirements 7

4 Installing InfoWatch Device Monitor 21

4.1 Deployment Scheme for InfoWatch Device Monitor 21

4.2 InfoWatch Device Monitor Server End Setup 24

4.2.1 Database Deployment Managed by Microsoft SQL Server DBMS 24

4.2.2 Database deployment managed by Oracle DBMS 25

Configuring InfoWatch Device Monitor connection to Oracle DBMS server 25

4.2.3 Database Deployment Managed by PostgreSQL DBMS 26

4.2.4 Server Setup Recommendations 27

Account for launching InfoWatch Device Monitor Server 27

Enhancing performance 28

4.2.5 InfoWatch Device Monitor Server End Installation Procedure 28

4.3 InfoWatch Device Monitor Agent Installation 38

4.3.1 Installation methods 38

4.3.2 Preparation 38

4.3.3 Local Installation of Agent on Workstation running Windows OS 41

Installing Device Monitor Agent on the computer with OS Microsoft Windows using MSI package followed by manual input of parameters: 42

Installing Device Monitor Agent on the computer with OS Microsoft Windows using cmd package containing installation parameters: 42

Installing Device Monitor Agent on the computer with OS Microsoft Windows using MSI package in silent mode: 43

4.3.4 Local Installation of Agent on Workstation running Linux Family OS 46

4.3.5 Local Installation of Agent on Workstation running Mac OS 49

4.3.6 Agent Installation via Software Distribution Tools 50

5 Configuring InfoWatch Device Monitor Server 56

5.1 <applicationSettings> Section 57

5.1.1 <InfoWatch.DeviceMonitor.Server.Core.Properties.Settings> 57

5.1.2 <InfoWatch.DeviceMonitor.Server.Database.Properties.Settings> 58

5.1.3 <InfoWatch.DeviceMonitor.Server.Gui.Properties.Settings> 59

5.1.4 <InfoWatch.DeviceMonitor.Server.Client.Properties.Settings> 59

5.1.5 <InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings> 61

5.1.6 <InfoWatch.DeviceMonitor.Database.Core.Properties.Settings> 61

5.1.7 <InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings> 62

5.1.8 <InfoWatch.DeploymentSubSystem.Properties.Settings> 63
5.2 <system.diagnostics> Section 63
5.2.1 <trace> element 64
5.2.2 <sources> element 64
Element attributes 64
<listeners> element 64
5.2.3 <switches> element 65
5.3 Deleting Device Monitor temporary files 66
5.4 Configuring protection against guessing for Device Monitor 66
5.5 Configuring validation of the remote server certificates 67
5.5.1 Validation of the remote server certificates when starting a remote SSL session 68
Default values 68
5.5.2 Certificate of the Traffic Monitor XAPI service 68
5.5.3 Traffic Monitor web-server certificate 69
5.5.4 Certificate of the Platform EPEVENTS service 70
5.5.5 View Logs 70
6 Updating InfoWatch Device Monitor 71
6.1 Updating InfoWatch Device Monitor Server End 71
6.2 Updating InfoWatch Device Monitor Agent 74
7 Uninstalling InfoWatch Device Monitor 76
7.1 Uninstalling InfoWatch Device Monitor Agent 77
7.1.1 Centralized Uninstallation of Agent 77
Uninstalling using Device Monitor Management Console 77
Uninstalling Agent installed via software distribution tools 78
7.1.2 Local Uninstallation of Agent on Workstation running Windows OS 78
Uninstalling Agent using "Programs and Features" Tool 78
Uninstalling Agent using Microsoft Program Install and Uninstall Troubleshooter 78
Uninstalling Agent using Windows Management Instrumentation (WMI) 79
Uninstalling Agent using Windows Management Instrumentation (WMI) and PsExec tool 79
7.1.3 Local Uninstallation of Agent on Workstation running Linux Family OS 80
Uninstalling using script 80
Uninstalling using OS 81
7.1.4 Local Uninstallation of Agent on Workstation running Mac OS 81
8 Appendix A. Username and Password Recommendations 82
9 Configuring Access Network Rules 84

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/System or Device Monitor) – software intended to intercept data in company information traffic.

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.

Associated documentation for InfoWatch Activity Monitor includes the following:

- «InfoWatch Activity Monitor. Installation Guide». The document describes how to install, update, uninstall Activity Monitor.
- «InfoWatch Activity Monitor. Administration Guide». The document describes how to configure and prepare Activity Monitor for work.
- «InfoWatch Activity Monitor. User Guide». The document describes how to work in Activity Monitor.

3 Hardware and Software Requirements

Server Hardware requirements 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 Hardware and Software 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 the 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 11 and later ones.	• 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 **Important!** To enhance performance, follow the recommendations listed in the articles: • "Server Setup Recommendations" • "Database Deployment Managed by PostgreSQL DBMS" (if you are planning to use PostgreSQL DBMS)

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; • Microsoft Windows Server 2022; • Astra Linux Special Edition 1.7 in "Orel" (x64), "Voronezh" (x64) and "Smolensk" (x64) editions; • Astra Linux Special Edition 1.8 in "Orel" (x64), "Voronezh" (x64) and "Smolensk" (x64) editions;	• Local DNS is required to convert domain names into addresses • TLS 1.2 should be supported **Supported kernel versions of Astra Linux Special Edition 1.7 in "Orel", "Voronezh" and "Smolensk" editions** • 5.4.0-54-generic • 5.4.0-54-hardened • 5.4.0-81-generic • 5.4.0-81-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.4.0-186.astra2+ci2 (starting with version 7.15.2) • 5.10.0-1045-generic • 5.10.0-1045-hardened • 5.10.142-1-generic • 5.10.176-1-generic • 5.10.216-1.astra2+ci2 (starting with version 7.15.2) • 5.10.233-1-generic (starting with version 7.17.2)

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
			• RED OS 7.3; • RED OS 8.0; • Alt Workstation 10; • macOS Sequoia 15.1; • macOS Sequoia 15.2; • macOS Sequoia 15.3.	• 5.10.239-1-generic (starting with version 7.18.4) • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic • 5.15.0-70-hardened • 5.15.0-83-generic • 5.15.0-111-generic (starting with version 7.15.1) • 5.15.0-127-generic (starting with version 7.17.4) • 5.15.0-142-generic (starting with version 7.18.4) • 6.1.50-1-generic#astra2+ci6 (up to version 7.13.5) • 6.1.50-1-generic#astra4+ci68 (starting with version 7.13.6) • 6.1.90-1-generic (starting with version 7.15.1) • 6.1.124-1-generic (starting with version 7.17.2) • 6.1.141-1-generic (starting with version 7.18.4)

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				Supported kernel versions of Astra Linux Special Edition 1.8 in "Orel", "Voronezh" and "Smolensk" editions • 6.1.90-1-generic (starting with version 7.17.0) • 6.1.124-1-generic (starting with version 7.17.5) • 6.1.141-1-generic (starting with version 7.17.10) • 6.1.152-1-generic (starting with version 7.18.8) • 6.6.28-1-generic (starting with version 7.17.0) • 6.12.11-1-generic (starting with version 7.17.5) • 6.12.34-1-generic (starting with version 7.17.10) • 6.12.47-1-generic (starting with version 7.18.8) **Supported kernel versions of RED OS 7.3** • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				• 5.15.35-4 • 5.15.35-5 • 5.15.72-1 (starting with version 7.7.1) • 5.15.78-2 (starting with version 7.8) • 5.15.87-1 (starting with version 7.8.1) • 5.15.106-1 • 5.15.117-1 • 5.15.125-1 • 5.15.131-1 • 5.15.161-1 (starting with version 7.14.1) • 5.15.178-1 (starting with version 7.18.6) • 6.1.20-2 • 6.1.44-1 • 6.1.52-1 • 6.1.85-1 (starting with version 7.13.4) • 6.1.94-1 (starting with version 7.14.1) • 6.1.110-1 (starting with version 7.14.5) • 6.1.128-2 (starting with version 7.16.4) • 6.1.143-1 (starting with version 7.17.10) • 6.1.148-1 (starting with version 7.18.4) • 6.1.158-1 (starting with version 7.18.8)

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				Supported kernel versions of RED OS 8.0 • 6.6.6-1 (starting with version 7.17.0) • 6.6.26-1 (starting with version 7.17.0) • 6.6.34-1 (starting with version 7.17.0) • 6.6.51-1 (starting with version 7.17.0) • 6.6.76-1 (starting with version 7.17.0) • 6.12.21-1 (starting with version 7.17.3) • 6.12.37-1 (starting with version 7.17.10) • 6.12.56-1 (starting with version 7.18.8) **Supported kernel versions of Alt Workstation 10** • 5.10.133-std-def-alt1 • 5.10.135-std-def-alt1 • 5.10.136-std-def-alt1 • 5.10.163-std-def-alt1 • 5.10.164-std-def-alt1 • 5.10.165-std-def-alt1 • 5.10.168-std-def-alt1 • 5.10.170-std-def-alt1

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				• 5.10.172-std-def-alt1 • 5.10.174-std-def-alt1 • 5.10.176-std-def-alt1 • 5.10.177-std-def-alt1 • 5.10.179-std-def-alt1 • 5.10.182-std-def-alt1 • 5.10.185-std-def-alt1 • 5.10.186-std-def-alt1 • 5.10.191-std-def-alt1 • 5.10.194-std-def-alt1 • 5.10.195-std-def-alt1 • 5.10.197-std-def-alt1 • 5.10.198-std-def-alt1 • 5.10.199-std-def-alt2 • 5.10.200-std-def-alt1 • 5.10.203-std-def-alt1 • 5.10.204-std-def-alt1 • 5.10.205-std-def-alt1 • 5.10.206-std-def-alt1 • 5.10.207-std-def-alt1 (starting with version 7.12.1) • 5.10.208-std-def-alt1 (starting

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				with version 7.12.1) • 5.10.209-std-def-alt2 (starting with version 7.12.2) • 5.10.211-std-def-alt1 • 5.10.212-std-def-alt1 • 5.10.213-std-def-alt1 (starting with version 7.13.1) • 5.10.216-std-def-alt1 (starting with version 7.13.6) • 5.10.217-std-def-alt1 starting with version 7.13.9) • 5.10.218-std-def-alt1 (starting with version 7.13.10) • 5.10.219-std-def-alt1 (starting with version 7.14.1) • 5.10.220-std-def-alt2 (starting with version 7.14.1) • 5.10.221-std-def-alt1 (starting with version 7.14.2) • 5.10.223-std-def-alt1 (starting with version 7.14.3) • 5.10.224-std-def-alt1 (starting with version 7.14.4)

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				• 5.10.226-std-def-alt1 (starting with version 7.14.5) • 5.10.227-std-def-alt1 (starting with version 7.15.1) • 5.10.228-std-def-alt1 (starting with version 7.15.2) • 5.10.231-std-def-alt1 (starting with version 7.16.1) • 5.10.233-std-def-alt1 (starting with version 7.16.2) • 5.10.234-std-def-alt1 (starting with version 7.16.3) • 5.10.235-std-def-alt1 (starting with version 7.17.1) • 5.10.237-std-def-alt1 (starting with version 7.17.4) • 5.10.238-std-def-alt1 (starting with version 7.17.7) • 5.10.240-std-def-alt1 (starting with version 7.17.10) • 5.10.241-std-def-alt1 (starting with version 7.18.3) • 5.10.242-std-def-alt1

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				(starting with version 7.18.4) • 5.10.244-std-def-alt1 (starting with version 7.18.4) • 5.10.246-std-def-alt1 (starting with version 7.18.8) • 5.15.94-un-def-alt1 • 5.15.109-un-def-alt1 • 6.1.29-un-def-alt1 • 6.1.32-un-def-alt1 • 6.1.42-un-def-alt1 • 6.1.49-un-def-alt1 (starting with version 7.13.2) • 6.1.67-un-def-alt0.c10f.1 (starting with version 7.12.4) • 6.1.75-un-def-alt1 (starting with version 7.12.2) • 6.1.77-un-def-alt1 (starting with version 7.12.2) • 6.1.78-un-def-alt1 (starting with version 7.12.4) • 6.1.79-un-def-alt1 (starting with version 7.12.5) • 6.1.80-un-def-alt1

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				• 6.1.81-un-def-alt1 • 6.1.82-un-def-alt1 (starting with version 7.13.1) • 6.1.83-un-def-alt1 (starting with version 7.13.2) • 6.1.84-un-def-alt1 (starting with version 7.13.4) • 6.1.85-un-def-alt1 (starting with version 7.13.4) • 6.1.90-un-def-alt1 (starting with version 7.13.8) • 6.1.94-un-def-alt1 (starting with version 7.14.1) • 6.1.96-un-def-alt1 (starting with version 7.14.1) • 6.1.99-un-def-alt1 (starting with version 7.14.2) • 6.1.100-un-def-alt1 (starting with version 7.14.3) • 6.1.111-un-def-alt1 (starting with version 7.14.6) • 6.1.112-un-def-alt1 (starting with version 7.15.0)

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				• 6.1.113-un-def-alt1 (starting with version 7.15.1) • 6.1.115-un-def-alt1 (starting with version 7.15.2) • 6.1.119-un-def-alt1 (starting with version 7.16) • 6.1.121-un-def-alt1 (starting with version 7.16.1) • 6.1.123-un-def-alt1 (starting with version 7.16.1) • 6.1.124-un-def-alt1 (starting with version 7.16.2) • 6.1.127-un-def-alt1 (starting with version 7.16.3) • 6.1.128-un-def-alt1 (starting with version 7.16.3) • 6.1.130-un-def-alt1 (starting with version 7.17.1) • 6.1.131-un-def-alt1 (starting with version 7.17.1) • 6.1.132-un-def-alt1 (starting with version 7.17.2) • 6.1.140-un-def-alt1 (starting

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
				with version 7.17.4) • 6.1.141-un-def-alt1 (starting with version 7.17.7) • 6.1.144-un-def-alt1 (starting with version 7.17.10) • 6.1.146-un-def-alt1 (starting with version 7.17.10) • 6.1.147-un-def-alt1 (starting with version 7.18.1) • 6.1.148-un-def-alt1 (starting with version 7.18.3) • 6.1.151-un-def-alt1 (starting with version 7.18.4) • 6.1.153-un-def-alt1 (starting with version 7.18.4) • 6.1.157-un-def-alt1 (starting with version 7.18.6) • 6.1.158-un-def-alt1 (starting with version 7.18.8)
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;	

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
			• Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 and 8.1; • Microsoft Windows 10.	

Note:

* In case of working with a terminal session:

- RAM usage on a terminal server can reach short-term peaks up to 2.5 GB (approximately 850 MB for a single user session). Calculating RAM resources by a mean value for all users can help lower resource consumption to about 600-700 MB for a user session.
- RAM usage on a workstation can reach up to 1 GB. Limiting simultaneous configuration update on agents can help lower resource consumption to about 500-700 MB.

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".

Warning!

Device Monitor version 7.18.X is compatible with Activity Monitor version 3.4.X. Operation of Device Monitor version 7.18.X is not supported with earlier versions of Activity Monitor.

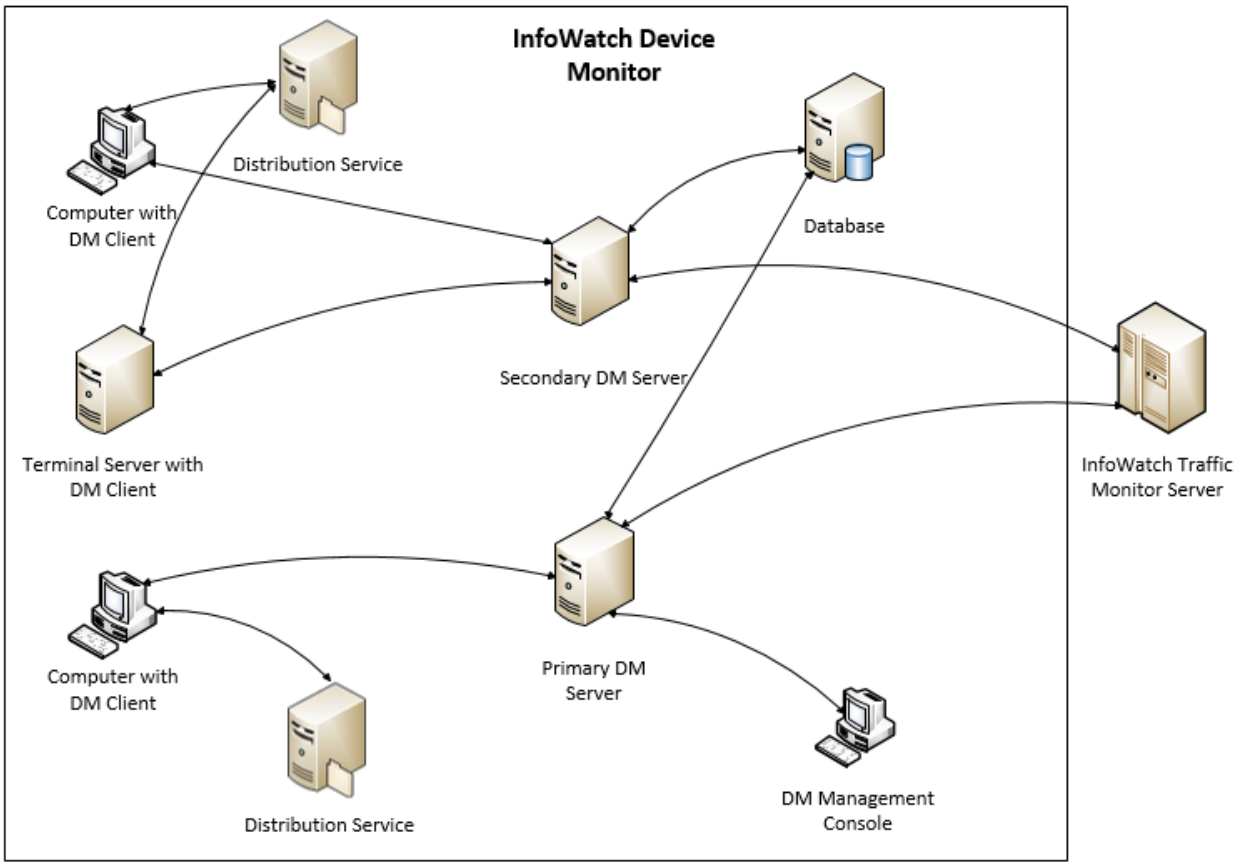
4.1 Deployment Scheme for InfoWatch Device Monitor

Find the InfoWatch Device Monitor components in the following table:

Component	Purpose
InfoWatch Device Monitor Client (InfoWatch Device Monitor client application, Agent)	Intercepts employees' actions on controlled computers
InfoWatch Device Monitor Server (InfoWatch Device Monitor server, Server)	Configures client applications, retrieves data from agents and sends it to InfoWatch Traffic Monitor, distributes deploy-agents to workstations
InfoWatch Device Monitor Database (Database)	Stores data that is required for the operation of Device Monitor
InfoWatch Device Monitor Management Console (Management Console)	Manages Device Monitor

Component	Purpose
Distribution service	Gets and stores the new version of Device Monitor Agent distibution kit
Servers Manager	Configures roles and other attributes of Device Monitor servers

The following image illustrates the interaction between the Device Monitor components:



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

You can host the server and the database on a single computer. However, to increase the performance, host the database and the 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. Install the **primary server** first (see the "*Infowatch Traffic Monitor. User Guide*" document, "InfoWatch Device Monitor Server Manager" article).
2. When you install the primary server, 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. You can install the **Management Console** 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 **distribution service** is installed together with the **primary Device Monitor server**, and has a repository with Agent distribution kits for the OS and platform being used. You can also install the service together with Device Monitor secondary servers.
7. Device Monitor Deploy Agents are distributed from the **primary server** to **workstations**. Then, the Deploy Agents download the Agent distribution kits from the specified distribution points of the nearest **distribution service**. Multiple workstations can download Agents simultaneously.
8. Agents connect to any available Device Monitor Server via an encrypted channel with binding to the Server by the key that 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 are subject to a security scheme rule and file 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 in the database. 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.
4. Provide the account with the right to start services.

If you are going 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

Before DBMS deployment

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.

Note:

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

DBMS deployment

Download PostgreSQL starting from version 11 from the official site and install it with default parameters.

When installing the application, the system will create `postgres` superuser. Create and enter a password for the user. To learn more about the user, open pgAdmin III utility, which is distributed in the installation package, and go to *Entrance roles* section.

After DBMS deployment

To enhance the System's response speed, change parameters in `postgresql.conf` configuration file:

- Assign 250 value to `"max_connections"` parameter.
- Configure log rotation.
- Specify other parameters which can optimize performance (memory resource consumption, WAL configuration, query planning). See official PostgreSQL documentation for details.

4.2.4 Server Setup Recommendations

Install Device Monitor Server and Device Monitor Agent 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.

Account for launching InfoWatch Device Monitor Server

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:

- **User**. Launch service on behalf of Windows domain account;
- **Network Service**. Launch service on behalf of account without administrator privileges on the workstation.

For Microsoft SQL Server DBMS database. If you select **Windows authentication** for database owner (see "Database deployment under Microsoft SQL Server DBMS"), select **User** option.

> **Important!**
>
> It is not recommended to select Network Service option. In this case, the user can obtain unlimited rights, which contradicts the security policy.
>
> In case you changed the account for an already started service, grant it write access to installation catalogue: `\Program Files\InfoWatch\Device Monitor\Server`.

Preparing Windows domain account

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 dialogue select **Local policies** > **Assign User Rights**.
- Double-click **Log on as service** in the right **Details** panel.
- 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.

Enhancing performance

To enhance the performance of Device Monitor:

- Place the Server, database and shadow copies on separate hard drives.
- In case of virtualization, place drives of virtual machines on different JBODs.
- Add the following directories to antivirus exceptions:
  - DBMS directory;
  - Directory for shadow copies;
  - `C:\Program Files\InfoWatch\Device Monitor`.
- In case you are planning to use PostgreSQL DBMS, follow the performance recommendations in "Database Deployment Managed by PostgreSQL DBMS" article.

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.

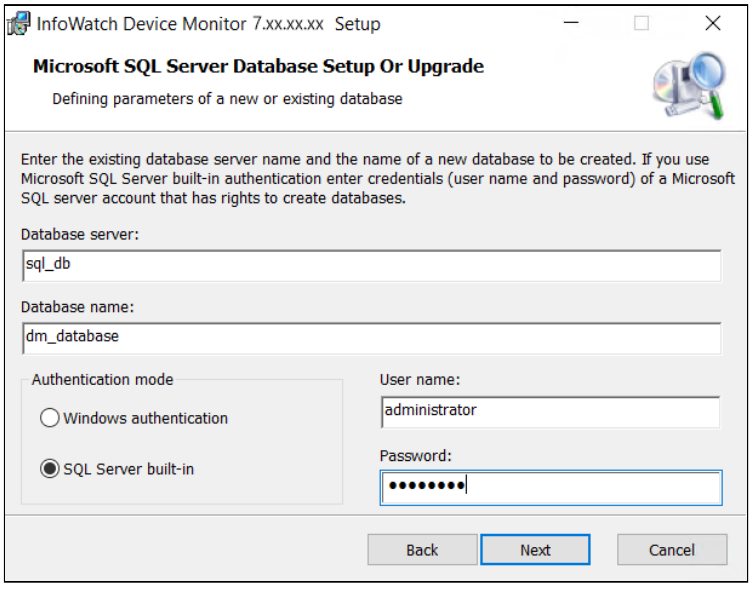
Click **Next**. In this case, all existing settings and elements of configuration will be replaced with imported ones.

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`

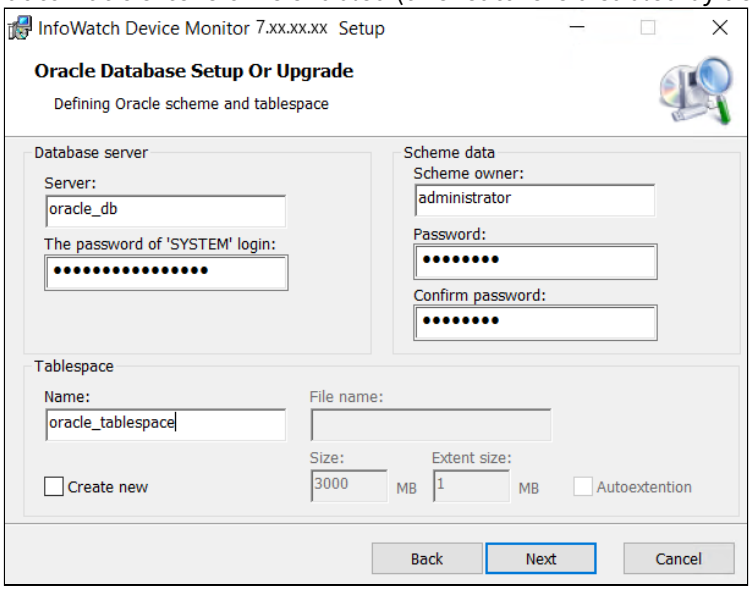
from the **tnsnames.ora** file or TNS string representation.
- **The password of 'SYSTEM' login**. SYSTEM account password.

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.

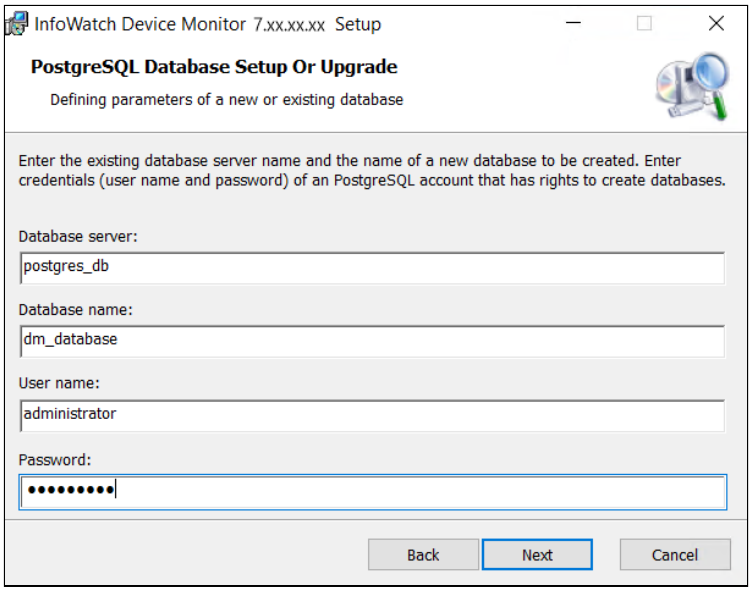
c. Configure tablespace settings in the **Tablespace** box.
You can use an existing tablespace or create a new one. If you are using an existing tablespace, enter the tablespace name in the **Name** field.
To create a new tablespace, check the **Create new** box. Then specify tablespace options:
- **Name**. 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**.

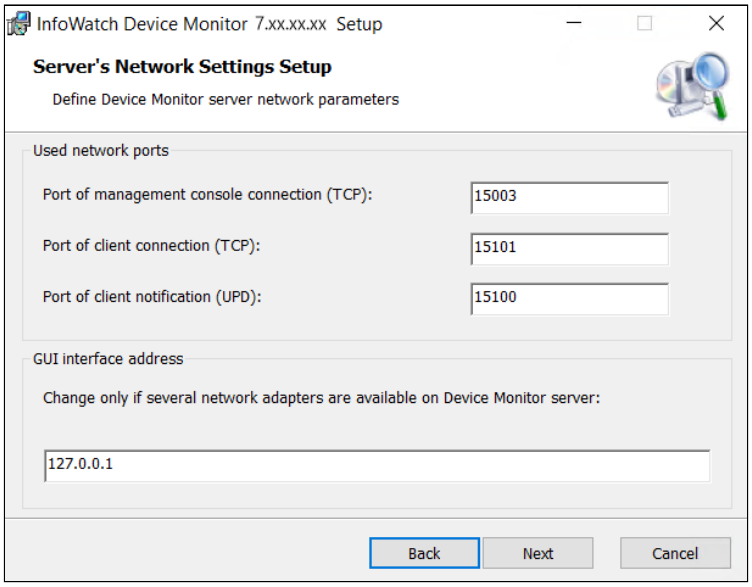
8. **Configuring the server**

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 InfoWatch 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**

    Warning!

For successful connection between Device Monitor Server and Traffic Monitor Server, you need to configure validation of the remote server certificates (for details, see "Configuring validation of the remote server certificates"). You can do it before or after the installation.

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).

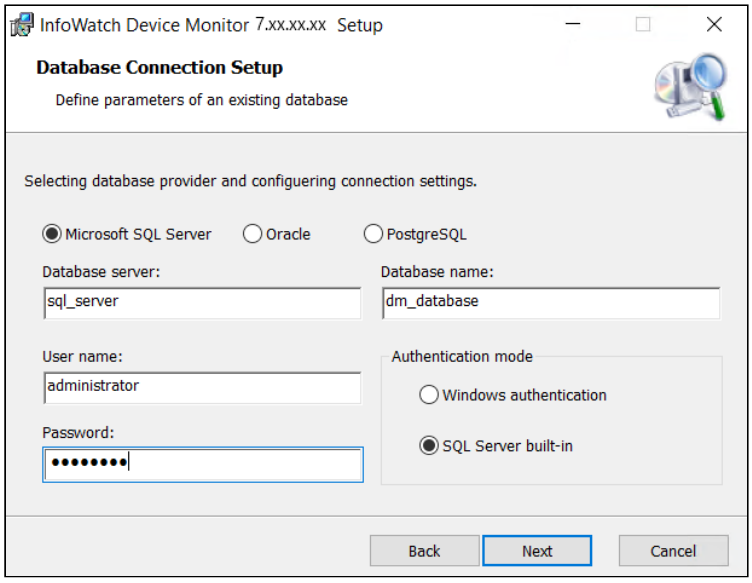
14. **Secondary server installation**
    Secondary server activity is based on primary one, primary server settings deploy in secondary server thus guarantying Device Monitor servers connection.

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

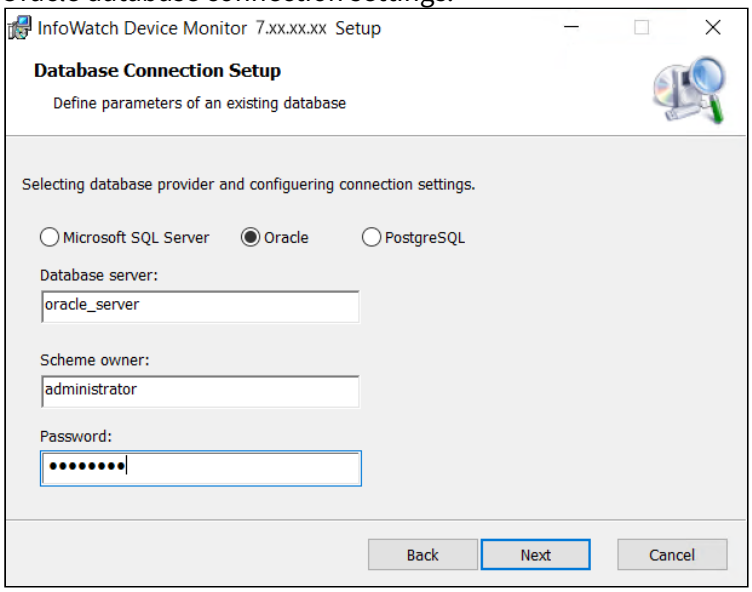
   You can change the list of components you want to install. All components are to be installed on one workstation by default. If you plan to use a Management Console or Distribution service on one workstation you do not need to install this feature: click **Management Console** or **Distribution service** 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.

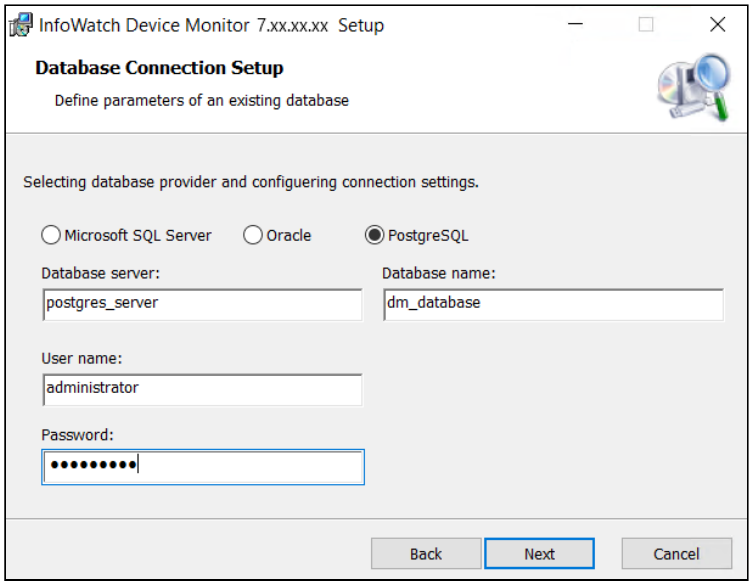
e. Database connection setup
   Specify DBMS managing Device Monitor database and put in the rest connection parameters that were used while installing the primary server.
   Microsoft SQL Server connection settings
   If the account uses Windows authentication, and the database was created by a domain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



Oracle database connection settings:

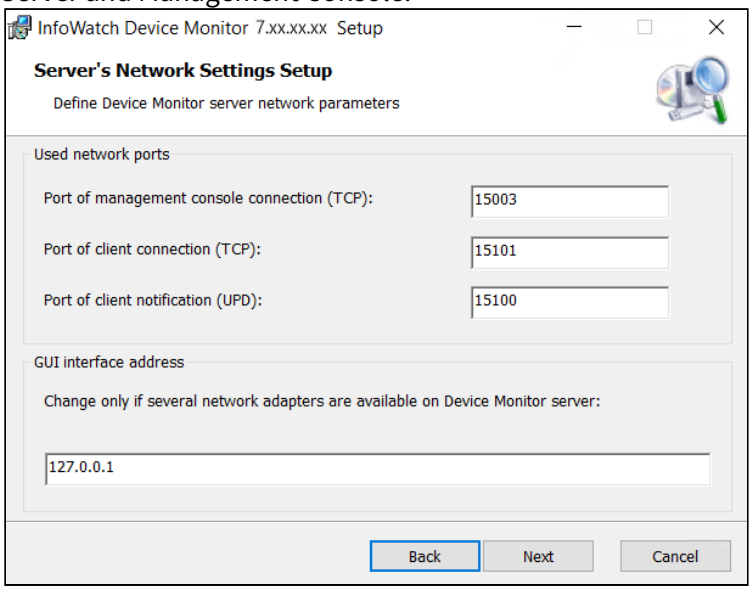


PostgreSQL database connection settings:



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. In this case, the event interception time will be displayed correctly.

> **Warning!**
>
> Please, do not install InfoWatch Device Monitor Agent and InfoWatch Device Monitor server on the same computer, as it may cause the server to fail.

4.3.1 Installation methods

You can install InfoWatch Device Monitor Agent on workstations in the following ways:

- Local Installation. It uses a universal installer to run installation on each computer:
  - Local Installation of Agent on Workstation running Windows OS;
  - Local Installation of Agent on Workstation running Linux Family OS;
  - Local Installation of Agent on Workstation running Mac OS;
- Remote installation using third-party software. It uses software distribution tools: for example, Microsoft Active Directory group policy;
- Installation via distribution tasks. It uses InfoWatch Device Monitor Management Console (for details, see "Agent Remote Installation, Updating and Uninstallation");
- Automatic installation. It uses InfoWatch Device Monitor Management Console (for details, see "Active Directory Connecting and Synchronizing").

4.3.2 Preparation

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 InfoWatch Device Monitor Agent processes to the list of security exceptions (you may find the list of files 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 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 `ftapihook654.dll` component version 3.2.4.1. (for details, see the "VmWare Horizon VDI compatibility issues" article).
6. Provide access to the ports that are required for operation of InfoWatch Device Monitor Agent (for details, see "Configuring Access Network Rules").
   To quickly obtain the FQDN of a workstation running Linux, be sure to configure the following parameters before installing the Agent:
   a. The `/etc/hostname` file contains:
      - host name, e.g. `computer-20`
        or

- FQDN, e.g. `computer-20.corp.ad`

b. The correspondence between the host name, FQDN and IP address is defined in the `/etc/hosts` file:
   - If the host name is determined on the workstation and the workstation has the FQDN, then the file must contain the following string:

     ```
     127.0.1.1 <FQDN name> <hostname>
     ```

     where `<FQDN name>` is the FQDN;
     `<hostname>` is the host name.
     For example, for the `computer-20` host name and `computer-20.corp.ad` FQDN, the string will look as follows:

     ```
     127.0.1.1 computer-20.corp.ad computer-20
     ```

   - If the workstation has no FQDN, then the file must contain the following string:

     ```
     127.0.1.1 <hostname>
     ```

   - If the `/etc/hostname` file contains the FQDN, then the file must contain the following string:

     ```
     127.0.1.1 computer-20.corp.ad
     ```

     Note:

     The IP address value can be equal to 127.0.1.1 or 127.0.0.1.

     Note:

     You can configure the listed parameters using third-party software, e.g. *Join to a domain*.

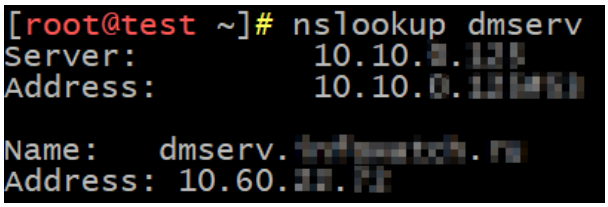
     To avoid errors when adding a host to the Active Directory, the host name must meet the following requirements:
     - You may use Latin characters (`A` - `Z` , `a` - `z`), numbers (`0` - `9`) and hyphens.
     - The name length must not exceed 15 characters.

7. For connection between InfoWatch Device Monitor server and the workstation where InfoWatch Device Monitor Agent is to be installed, their domain names must be correctly resolved by DNS server into IP addresses. Check it using the following command:

   ```
   nslookup <hostname>
   ```

As a result, a message containing address of the DNS server, FQDN of the workstation and its address will be displayed.
Example:

```
nslookup dmserv
```



If you have executed this command for InfoWatch Device Monitor server and the **`server can't find dmserv: SERVFAIL`** error message has been displayed, then the connection will not be established.

> **Note:**
>
> To establish connection between InfoWatch Device Monitor server and InfoWatch Device Monitor Agent, you can also add the following line to the `/etc/hosts` file on the workstation where InfoWatch Device Monitor Agent is to be installed:
>
> ```
> <Device_Monitor_server_IP_address> <Device_Monitor_server_hostname>
> ```

If you have difficulties when configuring the network parameters, please contact your System Administrator.

8. If you do not need the component to control network settings (control panel), disable this component when creating InfoWatch Device Monitor Agent 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 the test workstations during two or three days, continue the installation on workstations.

> **Important!**
>
> - Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.
> - 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.
> - If a workstation is connected to a corporate network remotely (via a VPN agent):
>   1. Add the VPN agent to the list of interception exceptions (including the network exceptions).
>   2. To install the Device Monitor Agent, connect the workstation to the corporate network locally.

3. After the installation, make sure the exception settings are correct. In this case, the workstation can be used for remote work again.

- During the Agent installation, the Mozilla Firefox, and Mozilla Thunderbird applications (if they are running) will be closed.
- InfoWatch Device Monitor Agent is started automatically after the installation. Before you restart the computer the Agent has limited functionality, which includes:
  - Interception of traffic sent via proxy server;
  - Network interception (when Agent is installed on OS Windows 8 and later);
  - Interception of copying data to external devices.

Important!

When installing the Agent on the workstation running **Windows 7 Service Pack 1** or **Windows 2008 R2 Server**:

- Install specific Windows updates. For details, see "Hardware and Software Requirements".
- The 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.

Important!

On Linux family OS:

- For correct operation of Agent functionality, reboot the computer.
- Do not remove or modify the accounts listed below on your own because this will result in inoperability of Device Monitor Agent:
  - `iwdm` – used by the main Device Monitor service
  - `iwdeployagent` – used by Device Monitor distribution service
  - `iwregistry` – currently not in use

  The accounts are created in the operating system during the Agent installation; they will be removed automatically during the Agent uninstallation.

4.3.3 Local Installation of Agent on Workstation running Windows OS

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.

Get an actual package for Agent installation and write it to an 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. **Run the Installation Wizard**
   Insert the external device containing Agent's distribution kit to computer drive. Then open the `Client` directory. In the catalogue find and run the package for deploying on the required platform according to the parameters specified while packages forming. For example, `InfoWatch.DeviceMonitor.Client.7.18.0.x64.msi`.

   > **Note:**
   >
   > Starting from **Device Monitor version 7.18.5** when **installing an Agent for the first time**, the installer verifies if the list of applications excluded from interception was provided. In case the list is not provided, this Agent installation is to be interrupted. In this case the log will contain a record as follows: `CustomAction GetExclusionsFromServerWithCheck returned actual error`.
   > Check can be disabled only when installing Agent via the command line.

   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. **Configure 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. **Complete the installation**
   Proceed to the **Confirm installation** screen and click **Next** to start the Agent installation. Follow the instructions to complete the installation. Reboot 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. **Create an installation package**
   Create an actual cmd package for Agent installation (see "*InfoWatch Device Monitor. User Guide. Creating Installation Package*") and write it to an external device.

2. **Enter Windows command line**
   Start the command line (`cmd.exe`) under the Administrator account.
3. **Run the script**
   a. Go to the catalogue containing the installation script:

   ```
   cd <path_to_script>
   ```

   b. Run the script by entering its full name, for example:

   ```
   InfoWatch.DeviceMonitor.Client.7.18.0.x64.msi.cmd
   ```

   c. The installation without graphic interface will start in silent mode and without notifications. Wait till the installation is compete, then the log file with detailed information will be created.

Installing Device Monitor Agent on the computer with OS Microsoft Windows using MSI package in silent mode:

To minimize involvement in the installation process, you can install Agent in the silent mode.

Before running the installer:

1. Insert the external device containing Agent's distribution kit to computer drive.
2. Run the command line (`cmd.exe`) on behalf of Administrator.
3. Go to the catalogue where the Agent distributive is, by running the command:

   ```
   cd <path_to_distributive>
   ```

See the list of key in the table below. You can use them to specify the product installation parameters.

Key	Description
`/quiet`	Running the installation without user interface displaying
`/i <installation_package_name>`	Running the installation using the specified file
`PREDEFINED_CLIENTDIR`	The directory where to install the product Default value: `"%ProgramFiles%\Infowatch\DeviceMonitor\Client"` **Important!** The path to catalogue can contain the following symbols: `0-9` , `a-z` , `A-Z` ,`:`,`.`,`_`,`-`,`\`,` ` In case the path has other symbols, then the Agent installation will be incorrect.

Key	Description
`UNINSTALL_PASSWORD_SHA1_HASH`	Hash value of the uninstallation password in the hexadecimal format, calculated by the SHA-1 algorithm. If you specify the parameter, then the Agent uninstallation is available only if the correct password is provided. **Important!** It is required to calculate the password hash value for the encoding Unicode UTF-16LE. Specify the hash value by using only capital letters and numbers.
`IWPROXYDN`	The string containing the domain name of proxy server root certificate on a workstation, used to issue certificates to intercept protected traffic. The name has to meet the X.509 standard and contain the CN (Common Name) field. The fields inside the name have to be divided by a comma. Default value: `"CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow"`
`SHOW_USER_NOTIFICATION`	Whether to notify the user that workstation reboot is required. Possible values: • `"#x01000000"` (default value) – to display a notification; • `"#x00000000"` – not to display a notification.
`WAITING_REBOOT_PERIOD`	Waiting time (in hours) until the Agent notifies the user that workstation reboot is required. Default value: `"0"`
`REBOOT_NOTIFICATION_PERIOD`	Time (in hours) till the hard reboot, during which the Agent notifies the user that workstation reboot is required. Possible values: • Integers from 0 to 1000; • `"-1"` (default value) – to set up endless notifications and not to perform hard reboot.
`REBOOT_NOTIFICATION_RATE`	The frequency (in minutes) with which the Agent sends the user a notification requesting reboot. By default, the Agent displays a notification every 10 minutes. **Note:** In case the parameter is not specified, the Agent displays the notification every 10 seconds.

Key	Description
`REBOOT_NOTIFY_MESSAGE`	Text of the notification that the Agent displays to inform the user that reboot is required. The message cannot exceed 255 symbols. Default text: `"Reboot is required as soon as possible"`
`FORCE_REBOOT`	Whether to display the final notification before hard reboot. Possible values: • `"0"` (default value) – to display the final notification; • `"1"` – not to display the final notification. **Important!** After the final notification, an employee has 5 minutes to finish their operations. In case you specify `"1"` and `REBOOT_NOTIFICATION_PERIOD` parameter implies hard reboot, the reboot will be executed unexpectedly for the employee.
`HIDE_CLIENT`	Whether to hide Device Monitor Agent presence on the workstation. Possible values: • `"#x01000000"` – to hide the Agent; • `"#x00000000"` (default value) – not to hide the Agent. **Important!** Decision not to inform about interceptors usage can contradict your country legislation. **Important!** If you specify `"#x01000000"`, the Agent will not display notifications that reboot is required.
`NOIWPROXY`	Whether to install the component of network traffic interception. Possible values: • `"0"` (default value) – to install the component; • `"1"` – not to install the component.
`NOIWNBG`	Whether to install the component of network control. Possible values: • `"0"` (default value) – to install the component; • `"1"` – not to install the component.
`SRVPOOL`	The list of Device Monitor servers to which the Agent can connect. The list should be of the format: `<Server>[;<Server>[;<Server>[{*};{*}...]]]`

Key	Description
	where `<Server>` = `<DNS server name>:<port number>` Parameter value example: `"dmserver:15101;"` In case the Agent cannot connect to the first server in the list, then it will try to connect to the next server, and so on. After connection to the server is established, the Agent will be bound to it.
`EXCL_REQUIRED`	Starting from **Device Monitor version 7.18.5** when **installing an Agent for the first time**, the installer verifies if the list of applications excluded from interception was provided. In case the list is not provided, this Agent installation is to be interrupted. In this case the log will contain a record as follows: `CustomAction GetExclusionsFromServerWithCheck returned actual error`. If you want to disable the check, add to running command the following option: `EXCL_REQUIRED = 0`.
`/lvp <log_file_name>`	Record data into the specified log file

To install InfoWatch Device Monitor Agent:

1. Run the Agent installation command using parameters in the command line.
   Installation command example:

```
%windir%\system32\msiexec.exe /quiet /i
InfoWatch.DeviceMonitor.Client.x64.ru.7.18.0.192.msi PREDEFINED_CLIENTDIR="%ProgramFiles%
\Infowatch\DeviceMonitor\Client" IWPROXYDN="CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO
InfoWatch,OU=TechDep,ST=Moscow" SHOW_USER_NOTIFICATION="#x01000000"
WAITING_REBOOT_PERIOD="48" REBOOT_NOTIFICATION_PERIOD="10" REBOOT_NOTIFICATION_RATE="1"
HIDE_CLIENT="#x00000000" FORCE_REBOOT="0" NOIWPROXY="0" NOIWNBG="0"
SRVPOOL="dmserver:15101;" /lvp InfoWatch.DeviceMonitor.Client.x64.ru.7.18.0.192.log
```

2. Wait until the installation is complete.
3. Reboot your computer.

4.3.4 Local Installation of Agent on Workstation running Linux Family OS

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.

Note:

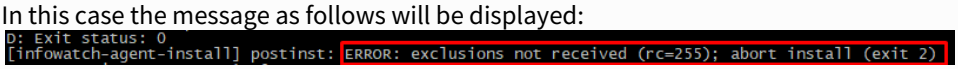
If your computer has a customized version of SeLinux system, we cannot guarantee correct installation of Agent.

1. **Preparing for the installation:**
   a. Make sure that the user on behalf of whom you will install Agent has required rights:
      - on computer running Alt Workstation 10 OS - rights to run `su`;
      - on computers with other Linux OS - sudoers privileges.
   b. Copy the archive with Device Monitor Agent installation and uninstallation package and scripts. The archive is a part of a distribution kit. A name of the archive depends on OS:
      - `Setup.AstraLinux-1.7-iwdm.x86_64.x.x.x.xx.tar.gz` - for Astra Linux Special Edition 1.7 OS;
      - `Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.tar.gz` - for RED OS 7.3;
      - `Setup.RedOS-8.0-iwdm.x86_64.x.x.x.xx.tar.gz` - for RED OS 8.0;
      - `Setup.AltLinux-10.0-iwdm.x 86_ 64.x.x.x.xx.tar.gz` - for Alt Workstation 10 OS,

      where `x.x.x.xx` is a build number.
      Next, we look at the example of installing Agent on RED OS 7.3. Installing on other supported OS is the same. Examples of commands for them are given below.
   c. Go to the directory to which you copied the archive and enter the unpacking command:
      `sudo tar -xvzf Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.tar.gz`
      As a result, the following files will be created: `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<agent_version>.deb`.
2. **Installing InfoWatch Device Monitor Agent:**
   a. Go to the directory where the content of the archive **`Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xxx.tar.gz`** is unpacked.
   b. To install the Agent, run the script by entering the command:
      - For common installation (in this case a network traffic interception component will be installed):
        `sudo ./install.sh <server>:<port>`
        where `<server>` is the IP-address or domain name of InfoWatch Device Monitor server,
        `<port>` is the 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`.

        Note:

        Starting from **Device Monitor version 7.18.5** when **installing an Agent for the first time**, the installer verifies if the list of applications excluded from interception was provided. In case the list is not provided, this Agent installation is to be interrupted. In this case the message as follows will be displayed:

        If you want to disable the check, add to running command the following option:
        `IW_EXCL_REQUIRED=0`.

        Example for how to install an Agent without check:

        `sudo IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101`

- For installation without a network traffic interception component:
  `sudo IWDM_NO_PROXY=1 ./install.sh <server>:<port>`

c. You can check the status of services by entering the following command:
`sudo systemctl status "iwdm*"`

> **Note:**
>
> If you have chosen not to install the network traffic interception component, then:
>
> - The `iwdmproxy` service will not be activated.
> - In the `/opt/iw/dmagent/etc/iwdmproxy` directory, the `no_proxy` file will be created.
> - When updating the Agent, the network traffic interception component will not be installed as well.

d. Reboot the workstation by running the command:
`reboot`

Examples of commands for other OS:

1. **Astra Linux OS:**

   a. Unpacking the archive:
   `sudo tar -xvzf Setup.AstraLinux-1.7-iwdm.x86_64.x.x.x.xx.tar.gz`
   b. Running installation:
   `sudo ./install.sh dm-server:15101`
   Example for how to install an Agent without exclusion list check:
   `sudo IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101`
   In case of installation without a network traffic interception component:
   `sudo IWDM_NO_PROXY=1 ./install.sh dm-server:15101`
   c. Checking the status of services:
   `sudo systemctl status "iwdm*"`

2. **Alt OS:**

   a. Unpacking the archive:

   ```
   tar -xvzf Setup.AltLinux-10.0-iwdm.x86_64.x.x.x.xx.tar.gz
   ```

   b. Running installation:

   ```
   su -c "./install.sh dm-server:15101"
   ```

   Example for how to install an Agent without exclusion list check:
   `su -c "IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101"`
   In case of installation without a network traffic interception component:

   ```
   su -c "IWDM_NO_PROXY=1 ./install.sh dm-server:15101"
   ```

   c. Checking the status of services:
   `su - -c 'systemctl status "iwdm*"'`

4.3.5 Local Installation of Agent on Workstation running Mac OS

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.

Important!

Installation via SSH connection is not supported.

1. **Preparing for the installation:**
   a. Make sure that the user on behalf of whom you will install Agent has `sudoers` privileges.
   b. Copy the archive with Device Monitor Agent installation and uninstallation package and scripts to the computer.
   In our example: `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`, where `x.x.x.xx` is the build number.
   c. Go to the directory to which you copied the archive and enter the unpacking command:

```
sudo tar -xvzf Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz
```

   As a result, the following files will be created: `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<agent version>.pkg`.
2. **Installing InfoWatch Device Monitor Agent:**
   a. Go to the directory with the content of **`Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`** archive.
   b. To install the Agent, run the script with the command:

```
sudo ./install.sh <server>:<port>
```

   In the command above:
   `<server>` is the IP address or domain name of InfoWatch Device Monitor server,
   `<port>` is the port to connect to InfoWatch Device Monitor server.
   In our example, the command is:

```
sudo ./install.sh dm-server:15101
```

   c. During installation, the script makes changes to operating system's trust certificate settings. Once you run the script, the operating system requests a permission in a separate window. For confirmation, enter the password for your account.
   Wait for the installation to complete. The product will be installed in `/opt/iw/dmagent` directory.
   d. Check the statuses of services by entering the following commands:

```
sudo launchctl print system/com.infowatch.iwdmproxy | grep state
```

```
sudo launchctl print system/com.infowatch.iwdmc | grep state
```

e. Reboot the workstation:

```
reboot
```

4.3.6 Agent Installation via Software Distribution Tools

> **Note:**
>
> Agent installation via software distribution tools is possible only on workstations running Windows OS or Linux family OS.

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

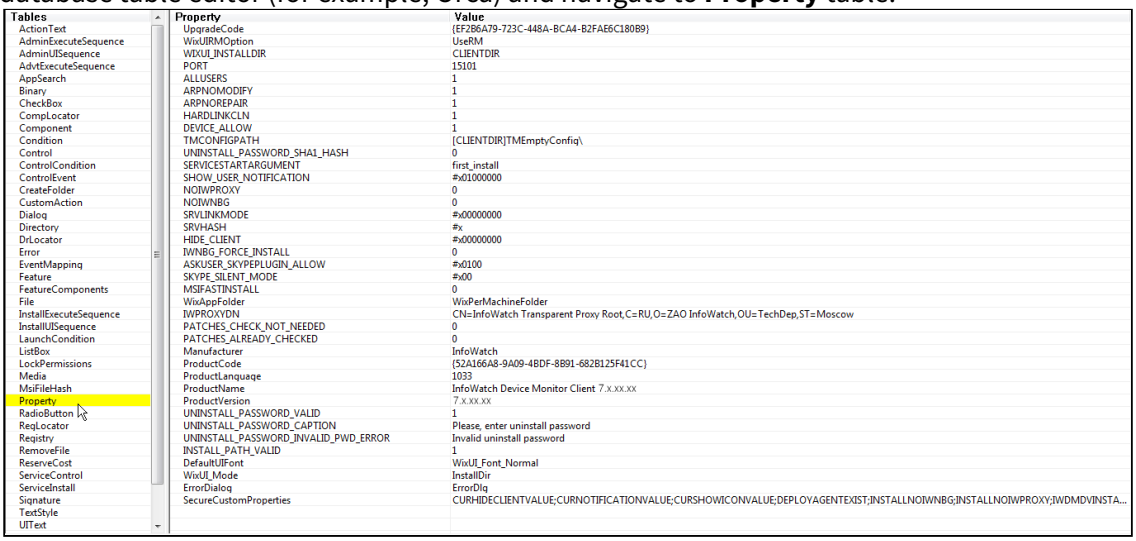
Agent installation from Microsoft Active Directory is carried out via group policy. To do so, you have to select a group policy that covers all target workstations. This policy may be assigned to:

- 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.7.18.0.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.

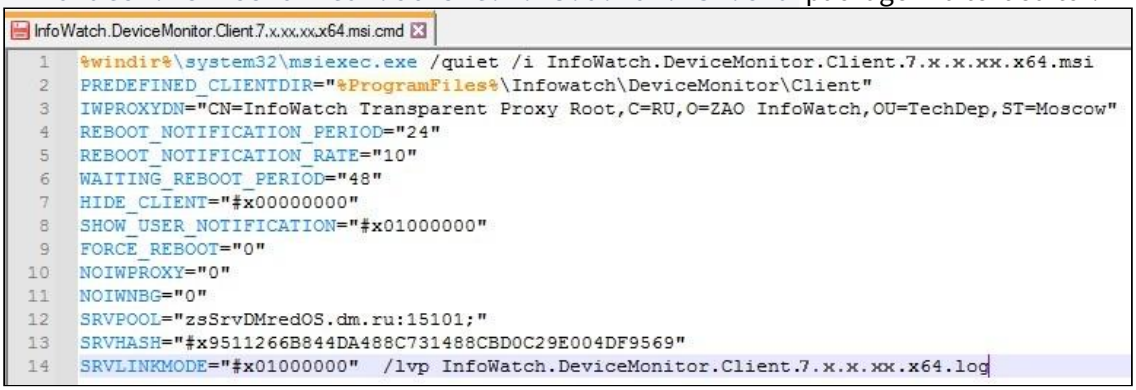
2. **Creating Transform File**

a. Open the `InfoWatch.DeviceMonitor.Client.7.18.0.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**.

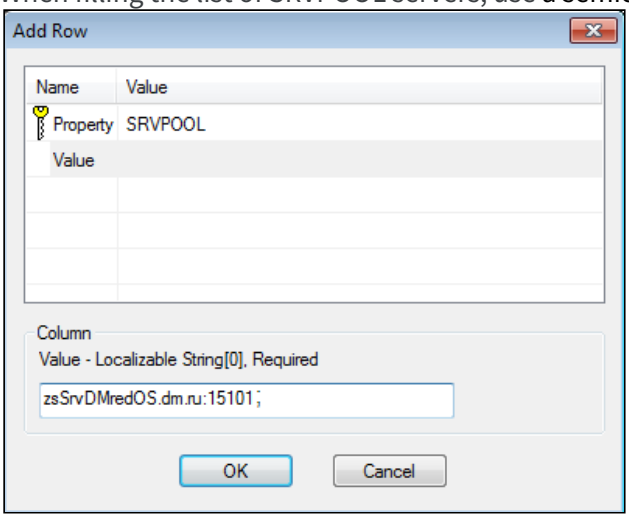
c. Open the previously created `InfoWatch.DeviceMonitor.Client.7.18.0.x64.msi.cmd` package in a text editor:



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**. When filling the list of SRVPOOL servers, use a semicolon ";" when listing:



> **Пример:**
>
> Starting from **Device Monitor version 7.18.5** when **installing an Agent for the first time**, the installer verifies if the list of applications excluded from interception was provided. In case the list is not provided, this Agent installation is to be interrupted. In this case the log will contain a record as follows: `CustomAction GetExclusionsFromServerWithCheck returned actual error`.
> If you want to disable the check, add the `EXCL_REQUIRED` property with a value of `0`.

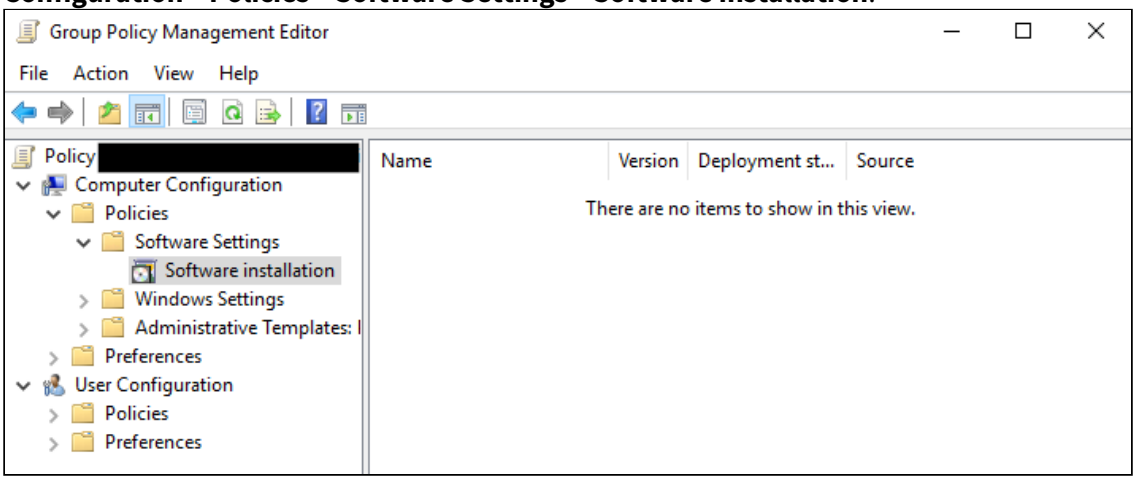
iii. To replace a property value, double-click the property value, enter the new value and press **Enter**.
Perform the steps above for all properties from the CMD package.

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

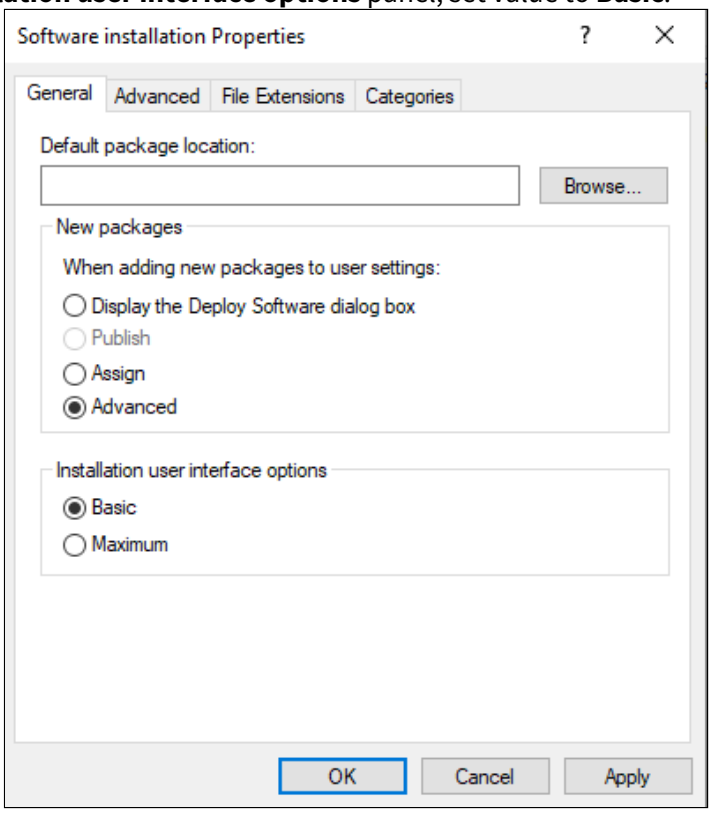
> **Note:**
>
> You can check the correctness of Agent installation on one of the workstations before proceeding to group policy editing.
>
> **Follow the steps:**
>
> i. Copy `*.msi` and `*.mst` installation files to one directory on the workstation. For example, to `C:\DM_Orca`.
> ii. Run the command line (`cmd.exe`) with administrator rights.
> iii. Go to the directory with the installation files:
> `cd C:\DM_Orca`
> iv. Run the command:
> `msiexec /qb /i <installation_file_name>.msi TRANSFORMS=<transformation_file_name>.mst /lvp <log_file_name>.log`
> v. Press **Enter** to run the installation process.
> vi. After the installation, reboot the system.
>
> In case of a successful installation, the Agent will be connected to the Server and displayed in DM Management Console.

3. **Editing Group Policy**
Edit group policy before installing Agent from Active Directory.
To edit group policy:
   a. Open **Group Policy Management Console** (**Start** > **Windows Administrative Tools** > **Group Policy Management**).
   b. In the console tree, select Active Directory container with all workstations, on which you plan to install Agent.
   c. Right-click the selected container and, in the window that opens, select **Create a GPO in this domain, and Link it here...** .
   d. Enter the name of the group policy object and click **OK**.
   e. In the right part of the window, open the **Linked Group Policy Objects** tab.
   f. Right-click the created group policy object and select **Edit**.

g. In the **Group Policy Management Editor** window that opens, select **Computer Configuration** – **Policies** – **Software Settings** – **Software Installation**.



h. Right-click **Software Installation** and select **Properties**.
i. In the window that opens, on the **General** tab, configure the following settings:
   - On the **New packages** panel, set value to **Advanced**;
   - On the **Installation user interface options** panel, set value to **Basic**.

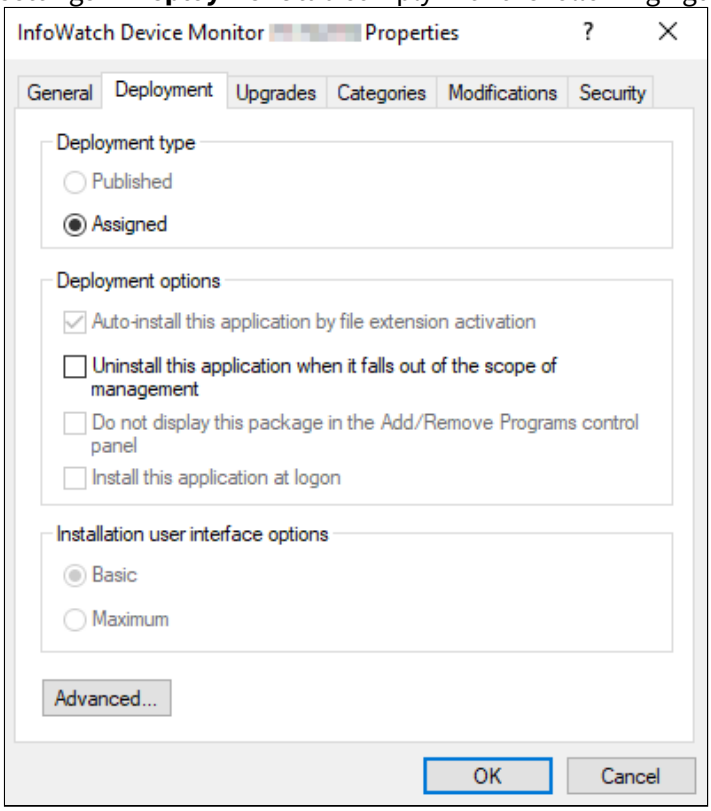


j. Click **Apply**.
k. Click **OK**.

4. **Preparing Agent installation task**

Agent installation task is created and configured in the **Group Policy Object Editor** window:

a. Select **Software Settings**.
b. Right-click the selected item and, in the pop-up menu, select **New** > **Package...** .
c. In the window that opens, specify the MSI installation package (it should be previously placed in the network directory that can be read by all target computers within the domain).
d. Click **Open**.
e. In the **Properties** window that opens:
    i. Make sure all settings in **Deployment** tab comply with the following figure:



    ii. On the **Modifications** tab, add the MST transform file (it should be previously placed in the network directory that can be read by all target computers within the domain).
    iii. After all necessary settings have been configured, click **OK**.
f. In the **Group Policy Object Editor** window, select **Computer Configuration** – **Policies** – **Administrative Templates:..** – **System** – **Scripts**.
g. In the right part of the window, select the **Run logon scripts synchronously** parameter.
h. Right-click it and select **Edit**.
i. In the parameter properties window that opens, select the check-box next to the **Enabled** value.
j. Click **Apply**.
k. Click **OK**.

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!

In case of updating the Agent on Linux OS, you must restart your workstation to ensure correct blocking of removable devices.

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 Panel. 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.

> **Note:**
>
> To ensure the correct operation of InfoWatch Device Monitor, configure access network rules on the computers, where Device Monitor components are installed. For details, see "Configuring Access Network Rules".

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.

Configuration section	Description
<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` is a setting name;
- `serializeAs` is 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>
```

Module parameters are described in the subsections:

- `<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings>`
- `<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings>`
- `<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>`
- `<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>`
- `<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>`
- `<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>`
- `<InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings>`
- `<InfoWatch.DeploymentSubSystem.Properties.Settings>`

5.1.1 `<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings>`

Server kernel configuration:

Parameter	Description
RemotingPort	TCP port processing Management Console service connections. Default value is `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.

Parameter	Description
	Default value is `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 is `300`

5.1.2 `<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings>`

Settings for database interaction module:

Parameter	Description
`DatabaseType`	Database types. Possible values: • `Oracle` • `Microsoft` • `PostgreSql`
`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 is `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 is `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 is `60`
`EventRelationStoredPeriod`	The interval in days. The parameter is used in formula to calculate the date of removal when cleaning up garbage events.

Parameter	Description
	Default value is `7`
`DeleteEventCount`	Maximum number of events to be deleted from the DB at a time. Default value is `10000`

5.1.3 `<InfoWatch.DeviceMonitor.Server.Gui.Properties.Settings>`

Management Console interface module settings:

Parameter	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 is `5`
`RenewOnCallTime`	Time (in minutes) for which a connection session with the Management Console is prolonged Default value is `2`

5.1.4 `<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>`

Settings of the module that serves client connections (controlled computers):

Parameter	Description
`Backlog`	Queue length of client connections waiting to be connected. Default value is `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:

Parameter	Description
	`C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir\<0÷255>\`
`DmpV1Adress`	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) • `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 is `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 is `700`
`Dmpv1ConnectionsQueueLengthAfterCut`	The number of connections after reducing the queue which exceeded the maximum size. Default value is `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 connection is established). Default value is `120`
`SSLPort`	The port number for encrypted connections. Default value is `15004`
`CheckUpdateTmConfigPeriodMinutes`	TM server query period (in minutes) checking for configuration changes. Default value is `30`

5.1.5 `<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>`

Basic settings for Traffic Monitor Server connector:

Parameter	Description
`DBPollTime`	Database query period (in milliseconds) checking for database events Default value is `10 000` Minimum value is `1000`, maximum value is `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 is `4`. Minimum value is `1`, maximum value is `32`.
`MaxSendEventCount`	The maximum number of events that is being read from DB at a time, to be sent to TM Default value is `1000` Minimum value is `1`, maximum value is `10000`.
`ShadowCopyTrasferBlockSize`	The size of a shadow copy data block sent to Traffic Monitor server, in MB. Default value is `16` Minimum value is `1`, maximum value is `64`.
`OperationTimeOutMs`	Waiting time for Traffic Monitor server response in milliseconds Default value is `0`, which means endless waiting Minimum value is `0`, maximum value is `1800000` (30 minutes) In case of an invalid value provided, the System uses the default value.

5.1.6 `<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>`

Settings of database low-level driver:

Parameter	Description
`CultureName`	Language of module diagnostic messages and other messages. Possible values: • `ru-RU` • `en-US`

Parameter	Description
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.

5.1.7 `<InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings>`

Settings of the module that interacts with Platform:

Parameter	Description
EPAddress, **EPToken**	Address of the Platform server and Platform token. The System does not use the values of these parameters.Specify Platform address and token in the Management Console (see "InfoWatch Device Monitor. User Guide", "Device Monitor Server Settings. Connecting to Platform Server").
DBPollTime	Frequency of the database poll (in ms). Default value is `5000` Minimum value is `5000`, maximum value is `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 is `1`, maximum value is `64`
MaxSendEventCount	The number of events that can be sent from the database at a time. Default value is `5000` Minimum value is `1`, maximum value is `10000`

Parameter	Description
RequestEventCount	The number of statistics events that can be sent as one batch. Default value is `100` Minimum value is `1`, maximum value is `10000`
WriteDisconnectEventLogIntervalMinute	Log file recording interval if the connection is broken or interrupted (in minutes). Default value is `60` Minimum value is `10`, maximum value is `240`
WaitPlatformDiskErrInitialMinute	Initial number of minutes to wait in case of error 507 before retrying to send events to Platform. Default value is `10` Minimum value is `1`, maximum value is `1440`
WaitPlatformDiskErrMaxMinute	Maximum number of minutes to wait in case of error 507 before retrying to send events to Platform. Default value is `60` Minimum value is `1`, maximum value is `1440`

5.1.8 `<InfoWatch.DeploymentSubSystem.Properties.Settings>`

Settings of the module that distributes (installation, update or removal) Agents and diagnostics:

Parameter	Description
NetworkLatency	Technical parameter, not recommended to change.
RunningInstallationsLimit	The maximum number of primary simultaneous installations on computers Default value is `0` (calculated according to formula)
BandwidthUsagePercentLimit	Controllable percent of network capacity the tasks can take Default value if no error or parameter specified is `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.

5.2.1 *<trace>* element

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

5.2.2 *<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 or uninstallation of the Agent.

Element attributes

`<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 diagnostics level of detail. Is always set to `System.Diagnostics.SourceSwitch` .

`<listeners>` element

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

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

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

- `<add>` . Add a new diagnostic messages receiver;
- `<remove>` . Delete diagnostic messages receiver.

<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 a 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 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" />
```

5.2.3 *<switches>* element

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

`<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.

5.5 Configuring validation of the remote server certificates

To improve security, Device Monitor Server is able to validate a remote server certificates. Such validation allows you to determine authenticity of the remote server when connecting to it.

Device Monitor validates the following certificates:

- XAPI service certificate – when connecting to the Traffic Monitor Server for sending events
- Traffic Monitor web server certificate (TMConfig certificate) – when connecting to Traffic Monitor Server for synchronization of data protection policies
- EPEVENTS service certificate – when connecting to the Platform Server for sending events

To successfully connect to the remote server for sending events:

1. Configure the certificate validation on the Device Monitor Server.
2. On the Device Monitor Server, install root certificates of the remote server into the root certificates store with the “local computer” level.

To successfully connect to the Traffic Monitor server for synchronization of data protection policies:

1. Configure the certificate validation on the Device Monitor Server.
2. If you want to use the built-in certificate of Traffic Monitor web server, go to step 5.
3. In your company's Certificate Authority, issue a X.509 certificate for the Traffic Monitor web server.
4. Configure the Traffic Monitor web server work with the issued certificate.

5. On the Device Monitor Server, install root certificates of the Traffic Monitor web server into the root certificates store with the “local computer” level.

5.5.1 Validation of the remote server certificates when starting a remote SSL session

To configure validation of the remote server certificates when starting a remote SSL session:

Set the values to `True` or `False` for the following fields of the SETTINGS table of the Device Monitor Server database:

- `IGNORE_SSLERR_TMXAPI_CONNECTION` – to ignore the Traffic Monitor XAPI service certificate validation
- `IGNORE_SSLERR_TMCONFIG_CONNECTION` – to ignore the Traffic Monitor TMConfig certificate validation
- `IGNORE_SSLERR_PLATFORM_CONNECTION` – to ignore the Platform EPEVENTS service certificate validation

If the value is `False`, the validation is not carried out.

Default values

The default values of the `IGNORE_SSLERR_TMXAPI_CONNECTION` field:

- when primarily installing Device Monitor Server – `False`, that is the Traffic Monitor XAPI service certificate validation is enabled
- when updating Device Monitor Server version 7.9 and earlier – `True`, that is the validation is disabled
- when updating Device Monitor Server version 7.10 and later – the value remains the same as before the update

The default values of the `IGNORE_SSLERR_TMCONFIG_CONNECTION` field:

- when primarily installing Device Monitor Server – `False`, that is the Traffic Monitor TMConfig certificate validation is enabled
- when updating Device Monitor Server – `True`, that is the validation is disabled

The default value of the `IGNORE_SSLERR_PLATFORM_CONNECTION` field:

- when primarily installing Device Monitor Server – `True`, that is the Platform EPEVENTS service certificate validation is disabled
- when updating Device Monitor Server version 7.9 and earlier – `True`, that is the validation is disabled
- when updating Device Monitor Server version 7.10 and later – the value remains the same as before the update

If the values of the `IGNORE_SSLERR_TMXAPI_CONNECTION`, `IGNORE_SSLERR_TMCONFIG_CONNECTION` and `IGNORE_SSLERR_PLATFORM_CONNECTION` parameters have been changed, restart Device Monitor Server service so that the certificate validation rules can take effect.

5.5.2 Certificate of the Traffic Monitor XAPI service

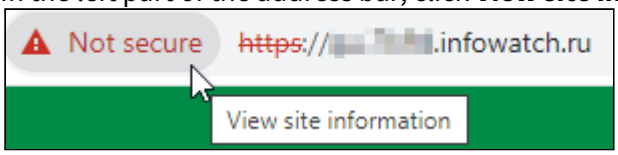
To install a certificate of the Traffic Monitor XAPI service:

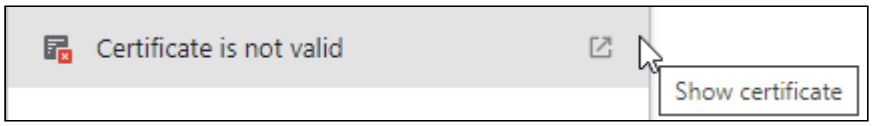
1. On the Traffic Monitor Server, open the `/opt/iw/tm5/etc/xapi.conf` file.

2. In the **ThriftServers** -> **xapi** section, find the `TrustedCertificatesPath` parameter.
   The value of this parameter contains the path to the root certificate and its name. If the path is not absolute, then it is relative to the `/opt/iw/tm5` directory.
   The `TrustedCertificatesPath` parameter value by default: `/opt/iw/tm5/etc/cert/trusted_certificates` .
3. Copy the root certificate to the computer on which Device Monitor Server is installed or is to be installed.
4. Rename the root certificate to `tmca.crt` .
5. Open the computer certificate manager snap-in. For this:
   a. From the **Start** menu, select **Run**.
   b. Enter `mmc` . Microsoft Management Console will open.
   c. From the **File** menu, select **Add or Remove Snap-ins**.
   d. In the opened dialogue box, from the **Available snap-ins** list, select **Certificates** and click **Add**.
   e. In the **Certificates Snap-in** dialogue box, select **Computer account** and click **Next**.
   f. In the **Select Computer** dialogue box, make sure that **Local computer** is selected and click **Finish**.
   g. In the **Add or Remove Snap-ins** dialogue box, click **OK**.
6. Go to the **Trusted Root Certification Authorities** -> **Certificates**.
7. In the **Action** menu, select **All Tasks** -> **Import**.
8. In the opened window, click **Next**.
9. Specify the path to the previously copied root certificate and click **Next**.
10. Make sure that **Place all certificates in the following store** -> **Trusted Root Certification Authorities** is selected and click **Next**.
11. Click **Finish**.

5.5.3 Traffic Monitor web-server certificate

To install a Traffic Monitor web-server certificate:

1. In your browser, open Traffic Monitor Management Console.
2. Export the Traffic Monitor web-server certificate from the browser, in our example it is Google Chrome. For this:
   a. In the left part of the address bar, click **View site information**.
   

   b. Click **Show certificate**.
   

   c. In the Certificate viewer, open the *Details* tab.
   d. Click **Export**.
   e. Click **Save**.
3. Copy the certificate to the computer on which Device Monitor Server is installed or is to be installed.
4. Follow the steps 5-11 of the Traffic Monitor XAPI service certificate installing instruction described above.

5.5.4 Certificate of the Platform EPEVENTS service

To install a certificate of the Platform EPEVENTS service:

1. On the Platform Server, get the `plca.crt` root certificate using the following command:
   `kubectl get secret -n infowatch epeventskeys-central -o 'go-template={{index .data "tls.crt"}}' | base64 -d > plca.crt`
   If Platform Server is not central in the cluster, then use the following command:
   `kubectl get secret -n infowatch epeventskeys-<node label> -o 'go-template={{index .data "tls.crt"}}' | base64 -d > plca.crt`
   where `<node label>` is a server node label.
2. Copy the root certificate to the computer on which Device Monitor Server is installed or is to be installed.
3. Follow the steps 5-11 of the Traffic Monitor XAPI service certificate installing instruction described above.

5.5.5 View Logs

If Device Monitor Server cannot validate the certificate, an error appears in logs. It contains information about the certificate and its status:

```
Can't validate TmXapi certificate. Chain error: Certificate thumbprint: <thumbprint> Subject: CN=XAPI,
OU=TD, O=InfoWatch, S=Moscow, C=RU

UntrustedRoot A certificate chain processed, but terminated in a root certificate which is not trusted by
the trust provider.

Certificate thumbprint: <thumbprint> Subject: CN=XAPI, OU=TD, O=InfoWatch, L=Moscow, S=Moscow, C=RU

UntrustedRoot A certificate chain processed, but terminated in a root certificate which is not trusted by
the trust provider.
```

You can configure time between sending error messages to logs using the `WRITE_SSLVERIFY_TMXAPI_LOG_INTERVAL`, `IGNORE_SSLERR_TMCONFIG_CONNECTION` and `WRITE_SSLVERIFY_PLATFORM_LOG_INTERVAL` fields of the SETTINGS table of the Device Monitor Server database. The default values of this fields are 3600 seconds. If the remote server certificate validation fails again and the time that passed from the last error message sending is less than the specified value, then a new error message is not sent.

To view logs:

1. Launch the **EventViewer** Windows Application.
2. Open the **Windows Logs** -> **Application** section.

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 InfoWatch Knowledge Base article "Compatibility among the versions of TM, DM and Agents".

Warning!

Device Monitor version 7.18.X is compatible with Activity Monitor version 3.4.X. Operation of Device Monitor version 7.18.X is not supported with earlier versions of Activity Monitor.

The System update is similar to its installation:

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

If you are using the main and secondary Device Monitor servers, they should not interact with the database during the upgrade process.
To update the System that consists of several servers:

1. Stop all Device Monitor servers being updated.
   To stop the server, you can manually stop the InfoWatch Device Monitor Server service on the Services tab of the Task Manager.
2. Update the main Device Monitor server followin the instruction.
   After the update, the installer automatically starts the server.
3. Update secondary Device Monitor servers.

Warning!

When transferring from Device Monitor server (Windows) version 7.14 and earlier ones, to Device Monitor server (Linux) version 7.15 and later, in case you need to continue working with the device control rules and the functionality of white lists, then it is required to install Device Control system and transfer these

rules and white lists. It is important to consider that the transfer is supported only for Postgres DBMS. If your version of Device Monitor server (Windows) is earlier than 7.13, then you need to update the server to the version 7.13 or 7.14 and then to transfer to Device Monitor server (Linux).

If you need to use the functionality of device control rules and white lists, then during the server update process select:

"Using Device Control is required, migrate rules and white lists". All device control rules and white lists existing in your system, will be transferred. It is important to consider that Device Control system installation is to be performed separately.

Otherwise, select:

"Using Device Control is not required, delete rules and white lists". All device control rules and white lists existing in your system, will be deleted.

Step 1. Start of 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. Configuring the database

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

Updating the database under Microsoft SQL Server DBMS

On the **Authentication mode** panel, select the authentication method for the user, who is updating the database. For this option, specify the authentication method which you selected while preparing the account (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 name and password into the **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 preparing the account, see the section "Database deployment under Microsoft SQL Server DBMS".

Update Database Under Oracle DBMS

In the **Database server** field, specify server name of the database.

In the **Scheme owner** and **Password** fields, specify database scheme owner name and password for scheme owner's account used for database update.

Update PostgreSQL Database

Enter the user name and password of the account that manages the updated database into the **User name** and **Password** fields.

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.

Important!

After you have updated Device Monitor server, you must re-enter or update passwords for synchronization with Active Directory and for primary distribution tasks (see the document "*InfoWatch Device Monitor. User Guide*", articles "*Active Directory Connecting and Synchronizing*" and "*Creating Primary Distribution Task*").

Note:

While updating Device Monitor server, the filters for displaying data in the Console (event filters, audit logs, etc.) that were configured for the previous version may not work.

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.

Important!

The Device Monitor Server and Agents that are installed on computers running Windows use the OpenSSL library for interaction. So if you previously manually enabled using the TLS 1.0/1.1 protocol on the Device Monitor Server, now you need to edit the configuration file in order to start using the TLS 1.2 protocol:

1. Make sure using TLS 1.2 is allowed in your browser properties.
2. Open the `C:\Program Files\InfoWatch\Device Monitor\Server\InfoWatch.DeviceMonitor.Server.exe.config` configuration file on the server.
3. Add the new value `Tls12` to the `ClientSecurityProtocols` parameters:

```
<setting name="ClientSecurityProtocols" serializeAs="String">
  <value>Tls;Tls11;Tls12</value>
```

4. Save the changes to the file.

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 in "InfoWatch Device Monitor Agent Installation" article.

You can use one of the following ways to update Device Monitor Agent on workstations running **Windows OS** or **Linux family OS**:

- 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).

Agents installed on workstations running **Mac OS** cannot be updated. Instead, uninstall Agent of the current version and install a later one.

To update Agents locally on computers running Linux:

1. Follow step 1 of the instruction for the local installation (see "Local Installation of Agent on Workstation running Linux Family OS").
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.

After the update:

- If Agent was stopped before the update, it will start automatically.
- Reboot the workstation, so that:
    - Applications started before the update could use the new interception mechanism;
    - Agents on workstations running Linux family OS could block external devices correctly and receive notifications.

7 Uninstalling InfoWatch 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.

For information on how to remove InfoWatch Device Monitor Agent, see "Uninstalling InfoWatch Device Monitor Agent".

7.1 Uninstalling InfoWatch Device Monitor Agent

The subsection contains possible methods of uninstalling InfoWatch Device Monitor Agent:

- Centralized Uninstallation of Agent
- Local Uninstallation of Agent on Workstation running Windows OS
- Local Uninstallation of Agent on Workstation running Linux Family OS
- Local Uninstallation of Agent on Workstation running Mac OS

It is recommended to uninstall Agents centrally. If you cannot do it, use the methods of local uninstallation.

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.

7.1.1 Centralized Uninstallation of Agent

Note:

Centralized uninstallation of Agent is possible only on workstations running Windows OS or Linux family OS.

There are the following methods of centralized uninstallation of InfoWatch Device Monitor Agent:

- Uninstalling using Device Monitor Management Console
- Uninstalling Agent installed via software distribution tools

Uninstalling using Device Monitor Management Console

To remove Agents centrally, you can create and run the uninstallation task in Device Monitor Management Console. This process is described in details in the "*Infowatch Device Monitor. User Guide*" document, the "Using Device Monitor Management Console → Agent Remote Installation, Updating and Uninstallation" section, the "Creating Uninstallation Task" article.

Uninstalling 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 remove the installation task from the group policy. 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, in the pop-up menu, select **All tasks** > **Remove**.
2. In the **Immediately uninstall software from users and computers** dialog window that opens, select **Remove software**.

   > **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 Agent installed on Astra Linux OS, RED OS or Alt OS:

1. First, update Agent via primary distribution task.
2. Run the product uninstalling task.

7.1.2 Local Uninstallation of Agent on Workstation running Windows OS

This subsection describes methods of local uninstallation of Agent on workstation running Windows OS:

- Uninstalling Agent using "Programs and Features" Tool
- Uninstalling Agent using Microsoft Program Install and Uninstall Troubleshooter
- Uninstalling Agent using Windows Management Instrumentation (WMI)
- Uninstalling Agent using Windows Management Instrumentation (WMI) and PsExec tool

Uninstalling Agent using "Programs and Features" Tool

If Agent is installed not in the hidden mode, then you can remove it in the following way:

1. In the search box on the taskbar, enter **control panel** and select **Control Panel** from the results.
2. Select **Programs** > **Programs and features**.
3. In the list, select **InfoWatch Device Monitor Client**.
4. Right-click the selected line and select **Uninstall**. Then follow the instructions on screen.

Uninstalling Agent using Microsoft Program Install and Uninstall Troubleshooter

You can use this method whether Agent is in the hidden mode or not, but only if an uninstallation password (a password that is required to uninstall the Agent) is not set.
It is recommended to use this method when:

- You cannot uninstall Agent using method listed earlier
- Agent and its parts may remain in the registry and/or file system
- You cannot install Agent on the workstation again.

To remove Agent:

1. Download the **Microsoft Program Install and Uninstall troubleshooter** tool from the official website.
2. Run the tool on the workstation where you want to uninstall Agent.
3. Select **Uninstalling** – **InfoWatch Device Monitor Client**.
4. Wait for the uninstallation to finish and reboot the computer.

Uninstalling Agent using Windows Management Instrumentation (WMI)

You can uninstall Agent using Windows Management Instrumentation (WMI). For this:

1. Run the command prompt (cmd.exe) as administrator.
2. Run Agent uninstallation with one of the following ways depending on uninstallation password setting:
   - If the password is not set, run the command:
     `wmic product where "Name like '%%Device Monitor client%%'" call uninstall`

     > **Note:**
     >
     > To run uninstallation in the silent mode, add the `/nointeractive` parameter to the command.
     >
     > If the password is set then you will be asked to enter it.

   - If the password is set:
     a. Find out an Agent identifier by running the command:
     `wmic product where "Name like '%%Device Monitor client%%'" get IdentifyingNumber`
     b. Run the Agent uninstallation command:
     `msiexec /x {<IdentifyingNumber>} /qn /lvp c:\Windows\dm.log UNINSTALL_PASSWORD=<password>`
     where `<IdentifyingNumber>` – the Agent identifier;
     " `/qn` " – parameter, hiding graphical interface msiexec. If you want to monitor the uninstallation process, use the " `/q` " parameter instead;
     " `/lvp c:\Windows\dm.log` " – optional parameter of logging Agent uninstallation. The " `c:\Windows\dm.log` " file is given as an example. You can specify any other one.
3. Wait for the uninstallation to finish. After that, the log file with the detailed information will be created. In the case of succesfull Agent uninstallation, the log file will contain a record of the following type: «Removal completed with status: 0».
4. Reboot the workstation.

Uninstalling Agent using Windows Management Instrumentation (WMI) and PsExec tool

This method repeats the previous one (see "Uninstalling Agent using Windows Management Instrumentation (WMI)"), but use **PsExec** tool and allows to remove Agent in case, when uninstalllation password is lost:

1. Download PsExec tool from the official website.
2. Place the downloaded file to the `C:\Windows\` directory.
3. Run the command prompt (cmd.exe) as administrator.
4. Find out an Agent identifier by running the command:
   `wmic product where "Name like '%%Device Monitor client%%'" get IdentifyingNumber`
5. Run the Agent uninstallation command:
   `PsExec.exe -i -s msiexec.exe /X {<IdentifyingNumber>} /q /lvp c:\Windows\dm.log`
   where `<IdentifyingNumber>` – the Agent identifier;
   " `/q` " – parameter, running the command in the silent mode, without user interaction;
   " `/lvp c:\Windows\dm.log` " – optional parameter of logging Agent uninstallation. The " `c:\Windows\dm.log` " file is given as an example. You can specify any other one.
6. Wait for the uninstallation to finish. After that, the log file with the detailed information will be created. In the case of succesfull Agent uninstallation, the log file will contain a record of the following type: «Removal completed with status: 0».
7. Reboot the workstation.

7.1.3 Local Uninstallation of Agent on Workstation running Linux Family OS

You can uninstall Agent on workstation running Linux family OS using the following methods:

- Uninstalling using script
- Uninstalling using OS

Uninstalling using script

To remove Agent:

1. Make sure that an archive containing Agent installation and uninstallation package and scripts is on the workstation. The archive is a part of a distribution kit. The archive name may differ depending on used OS for details see "Local Installation of Agent on Workstation running Linux Family OS".
   If necessary, copy the archive to the workstation and unpack it.

   > **Note:**
   >
   > On the workstation, the archive may be located in the `/tmp/iwdmupload/` directory.
   > As well, you can find it on the Device Monitor server, in the `C:\ProgramData\InfoWatch\SetupPackages` directory.

2. Go to the directory, where the archive is unpacked.
3. Run the script:
   `sudo ./remove.sh`
   Example of the command for Agent on Alt OS:
   `su -c "./remove.sh"`
   As a result, Device Moinitor Agent and distribution Agent will be removed.

Uninstalling using OS

If you cannot uninstall Agent using script, you can do it by running the following commands:

- On Astra Linux OS:
  `dpkg --purge iwdm`
  `dpkg --purge iwdeployagent`
- On RED OS and Alt OS:
  `rpm -e iwdm`
  `rpm -e iwdeployagent`

7.1.4 Local Uninstallation of Agent on Workstation running Mac OS

You can uninstall Agent on workstation running Mac OS with a script. For this:

1. Make sure that an archive containing Agent installation and uninstallation package and scripts is on the workstation. If necessary, copy the archive to the workstation and unpack it.
   In our example: `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`, where `x.x.x.xx` is the build number.
2. Go to the directory with the contents of the unpacked archive.
3. Run the script:

   ```
   sudo ./remove.sh
   ```

4. Reboot the workstation:

   ```
   reboot
   ```

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

9 Configuring Access Network Rules

Proper System operation requires that the below listed connections are allowed:

System component which requires the connection	Interaction between components		Port	Port's Function	
	Source	**Target**			
Device Monitor (DM) Server	DM Management console	DM Server	TCP 15003	Interaction between DM Server and Management Console	
	DM Agent	DM Server	TCP 15004	Protected connection between DM Server and Agents	Shadow copy transfer (encrypted channel)
	DM Agent	DM Server	UDP 15100		Agent notification
	DM Server	DM Agent			
	DM Agent	DM Server	TCP 15101		Shadow copy transfer
	DM Agent	DM Server	TCP 15200	Initiation of Agent distributive loading from DM Server to a workstation	
	DM Server	DM Agent	TCP 15505	Agent installation and uninstallation	
	DM Server	Platform	TCP 17104	Receiving data from InfoWatch Device Monitor (the setting is required for Activity Monitor)	
	Platform (central)	DM Agent	TCP 443	Receiving control commands (the setting is required for Activity Monitor)	
Agent running one of the Linux family OS	DM Server	Workstation	TCP 22	Agent installation	
Agent running Windows OS	DM Server	DM Agent	TCP 135		Remote Procedure Call (RPC) locator

	DM Server	DM Agent	UDP 137	Agent installation	NetBIOS Name Service
	DM Server	DM Agent	UDP 138		NetBIOS Datagram Service
	DM Server	DM Agent	TCP 139		NetBIOS Session Service
	DM Server	DM Agent	TCP 445		Sharing files required for Agent installation via SMB protocol
	DM Agent	DM Server			
	DM Server	DM Agent	TCP 593		RPC-over-HTTP
	DM Server	DM Agent	TCP 15506	Collecting logs, launching and stopping Agents	
	DM Agent	Activity Monitor Server	TCP 11008	Sending statistic events from Device Monior Agent directly to Activity Monitor (the setting is required for Activity Monitor)	
	DM Agent	Activity Monitor Sever	TCP 11006	Online monitoring (audio and video) - connection to workstation desktop. The setting is required for Activity Monitor	

Note:

In case different ports were appointed during installation:

- Use the appointed ports instead of the ones listed in the table;

or

- Replace the appointed ports with the ones listed in the table:

a. Stop the DM Server service with Task Manager or by running the command in cmd: `net stop iwdms`
b. To change DM Server and Agent connection ports, in the table `ServerOption` of the DM server database, edit the parameters:
   - `NotificationPort` (UDP 15100);
   - `ClientFacadePort` (TCP 15101);
   - `SSLPort` (TCP 15004).
c. To change Management Console connection port, in `C:\Program Files\InfoWatch\Device`

`Monitor\Server\InfoWatch.DeviceMonitor.Server.exe.config` file, edit the value of `DefaultPort` parameter (TCP 15003).

d. Restart DM Server service with Task Manager or by running the command in cmd: `net start iwdms`