

INFOWATCH

InfoWatch Device Monitor for Linux. Installation Guide

12/11/2026
© 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 Technical support 7

4 Hardware and Software Requirements 8

4.1 Hardware requirements 8

4.2 Software requirements 8

5 Installing InfoWatch Device Monitor 19

5.1 Distribution kit contents 19

5.2 Deployment Scheme for Device Monitor 19

5.3 Preparing the Environment 22

5.3.1 Examples of installing additional packages 29

Example of installing .NET on ALT OS 29

Example of installing .NET on Astra Linux 29

Example of installing .NET on Astra Linux 30

Example of installing conntrack and socat on RED OS 31

5.4 New Installation 31

5.4.1 "All-in-one" installation mode 32

5.4.2 Distributed installation of Device Monitor 36

5.4.3 Installation of a secondary server 40

5.4.4 Preparing the Device Monitor Server for Migration from Windows to Linux-based Operating Systems 42

5.5 Configuring Validation of the Remote Server Certificates 43

5.5.1 Verifying the certificates of remote servers when establishing an SSL session 43

5.5.2 Installing the Traffic Monitor XAPI service certificate 44

5.5.3 Installing the certificate of the Traffic Monitor web server 45

5.5.4 Installing the EPEVENTS Platform service certificate 46

5.5.5 Viewing logs 46

5.6 Installing Device Monitor Agents 46

5.6.1 Methods for installing the Device Monitor Agent 47

5.6.2 Preparing for installation 47

5.6.3 Local Installation of the Agent on a Workstation Running Windows 51

Installing the Device Monitor Agent on a computer running Microsoft Windows using an MSI package, followed by manual input of parameters 51

Installing the Device Monitor Agent on a computer running Microsoft Windows using an MSI package in silent mode 52

5.6.4 Local Installation of the Agent on a Workstation Running a Linux OS 55

Examples of commands for other operating systems 58

Installing the Agent on a workstation running MOS 59
5.6.5 Local Installation of the Agent on a Workstation Running Mac OS 59
5.6.6 Installing Agents Using a Distribution Task 61

6 Configuring Network Access Rules 63

7 Updating Device Monitor 68

7.1 Updating Device Monitor Server 68

7.2 Updating Device Monitor Agents 76

7.3 Updating Configuration on Device Monitor Agents 77

8 Uninstalling Device Monitor 81

8.1 Uninstalling the Web Interface and the Device Monitor Server 81

8.2 Uninstalling Device Monitor Agents 82
8.2.1 Local Uninstallation of an Agent on a Workstation Running Windows OS 82
Uninstalling Agent using "Programs and Features" Tool 82
Uninstalling Agent using Microsoft Program Install and Uninstall Troubleshooter 82
Uninstalling Agent using Windows Management Instrumentation (WMI) 82
Uninstalling Agent Using Windows Management Instrumentation (WMI) and PsExec Tool 83
8.2.2 Local Uninstallation of an Agent on a Workstation Running a Linux Family OS 84
Uninstalling with a script 84
Uninstalling using OS tools 84
8.2.3 Local Uninstallation of an Agent on a Workstation Running Mac OS 84

This guide contains information on how to install the components of InfoWatch Device Monitor for Linux (also referred to as the System, or Device Monitor).

1 Who should read this guide

This guide is intended for implementation engineers and security officers who will be working with the System and administering it. The guide is designed for users who are familiar with the basics of the Linux OS environment and the PostgreSQL DBMS.

2 Set of documents

The documentation package includes the following:

- InfoWatch Device Monitor for Linux. Installation Guide. The document contains a description of the process for installing the Server, Web-console, and Agents that are part of the System.
- InfoWatch Device Monitor for Linux. User Guide. Contains a description of how to work in the Web-console to solve tasks.

Related documentation for InfoWatch Traffic Monitor (also referred to as Traffic Monitor) includes:

- InfoWatch Traffic Monitor. Installation Guide. The guide describes how to install, configure, update, and uninstall the InfoWatch Traffic Monitor system.
- InfoWatch Traffic Monitor. Administration Guide. The guide describes how to administrate the InfoWatch Traffic Monitor system (database, server side).
- InfoWatch Traffic Monitor. User Guide. The guide contains the description of working with InfoWatch Traffic Monitor (configuration setup, data export/import, policy preparation for object processing).
- InfoWatch Traffic Monitor. Configuration Files Guide. Contains explanations for commonly used configuration files.

In addition to the primary System User Guide and Administration Guide, a Knowledge Base is available at lk.infowatch.ru, which includes troubleshooting materials and answers to questions. If you do not have access to the Knowledge Base, contact the InfoWatch technical support at support@infowatch.com

3 Technical support

If you cannot resolve issues that arise when using the System or have questions regarding the use of the System, you can contact the technical support:

- if you purchased the product from an InfoWatch partner, contact the technical support of this partner company;
- if you purchased the product directly from InfoWatch, you can contact our technical support at support@infowatch.com

You can also visit online support on our website: https://www.infowatch.ru/services/support

4 Hardware and Software Requirements

4.1 Hardware requirements

Server hardware requirements are defined based on the estimated load on the System and parameters of the network where the System is deployed. Estimated minimal hardware requirements are listed in the following table. We strongly recommend you to make a detailed configuration calculation with the assistance of InfoWatch experts or specialists of the partner company from which you have purchased the product.

Type	Requirements
Device Monitor server	
Disk subsystem	Not less than 100 GB of free space for installation. You also need space for data analysis. The size depends on server's load.
Processor	From 4 cores (frequency – 3.1 GHz, bit width – 64 bits, with support for SSE 4.2 instructions).
RAM	From 16 GB.
Device Monitor Management Console	
Disk subsystem	Not less than 100 GB free space required for installation.
Processor	From 2 cores (frequency – 1.1 GHz, bit width – 64 bits, with support for SSE 4.2 instructions)
RAM	From 16 GB, with an additional 1 GB per browser tab.
Device Monitor Agent for workstations	
Disk subsystem	At least 1 GB of free space for installation. Also the free space is required for temporary storage of files which are to be sent for analysis.
Processor	From 2 cores.
RAM	From 2.5 GB*.

Note:

* In case agents work 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 consumption on the user's workstation can reach 1 GB. Applying settings to limit simultaneous configuration updates by agents can reduce resource consumption to 500–700 MB.

4.2 Software requirements

Software requirements are listed in the table below:

Software	Additional requirements
Device Monitor server	

Software	Additional requirements

Operating system *(Server installation on the host, Host mode)*:
• Astra Linux Special Edition "Smolensk", versions:
  • 1.7.1.0 – 1.7.9.46
  • 1.8.1.0 – 1.8.5.46
• Astra Linux Special Edition "Orel", versions:
  • 1.7.1.0 – 1.7.9.46
• Astra Linux Special Edition "Voronezh", versions:
  • 1.7.1.0 – 1.7.9.46
• Astra Linux Special Edition version 1.8.5, certified
• RED OS, versions:
  • 7.3.3 – 7.3.6
  • 8.0.0
• ALT Linux OS, options:
  • SP Server 10.1.0 – 10.2.0
  • Server 10.1.0 – 10.2.0
You can install the Device Monitor server *with containerization support (Container mode)* on any OS where `podman` can be installed.
 	
The installation of a server with containerization support is guaranteed in the following **operating systems**:
• Astra Linux Special Edition "Smolensk", versions:
  • 1.7.1.0 – 1.7.9.46
  • 1.8.1.0 – 1.8.5.46
• Astra Linux Special Edition "Orel", versions:
  • 1.7.1.0 – 1.7.9.46
• Astra Linux Special Edition "Voronezh", versions:
  • 1.7.1.0 – 1.7.9.46
• Astra Linux Special Edition version 1.8.5 certified
• Red Hat Enterprise Linux, versions:
  • 7.6 – 7.9
  • 8.4 – 8.10
• Oracle Linux, versions:
  • 7.6 – 7.9
  • 8.4 – 8.10
• RED OS, versions:
  • 7.3.3 – 7.3.6
  • 8.0.0
	• Autostart for `iw_xapi_xapi` process should be enabled on the Traffic Monitor server.
	• Local DNS is required to convert domain names into addresses.
	• FIPS mode should be disabled.
	• TLS 1.2 should be supported.
	• If agents are to be distributed to workstations running Windows, a Samba client must be installed on the server.
	Important! To enhance performance, follow the recommendations listed in the articles:
	• Deployment Scheme for Device Monitor
	• Preparing the Environment

Software	Additional requirements

• ALT Linux OS, versions:
  • Server 10.1.0 – 10.2.0
  • Workstation 10.1.0 – 10.2.0
  • SP Server 10.1.0 – 10.2.0
  • SP Workstation 10.1.0 – 10.2.0
• Mos.OS Server Arbat 15.5
DBMS *(both installation modes)*: PostgreSQL versions 11 and later	

Platform-based web interface	

Operating system:
• Astra Linux Special Edition "Smolensk", versions:
  • 1.7.1.0 – 1.7.9.46
  • 1.8.1.0 – 1.8.5.46
• Astra Linux Special Edition "Orel", versions:
  • 1.7.1.0 – 1.7.9.46
• Astra Linux Special Edition "Voronezh", versions:
  • 1.7.1.0 – 1.7.9.46
• Astra Linux Special Edition version 1.8.5, certified
• Red Hat Enterprise Linux, versions:
  • 7.6 – 7.9
  • 8.4 – 8.10
• Oracle Linux, versions:
  • 7.6 – 7.9
  • 8.4 – 8.10
• RED OS, versions:
  • 7.3.3 – 7.3.6
  • 8.0.0
• ALT Linux OS:
  • Server 10.1.0 – 10.2.0
  • SP Server 10.1.0 – 10.2.0
  • Workstation 10.1.0 – 10.2.0
  • SP Workstation 10.1.0 – 10.2.0
• Mos.OS Server Arbat 15.5
Browser:
• Google Chrome
• Yandex Browser
	The browser must have hardware support for WebGL/ WebGL2.

Device Monitor Agent for workstations	

Software	Additional requirements

Operating system:
• Microsoft Windows, versions:
  • 7 Service Pack 1[1]
  • 8
  • 8.1
  • 10
  • 11
• Microsoft Windows Server, versions:
  • 2008 R2[1]
  • 2012
  • 2012 R2
  • 2016
  • 2019
  • 2022
• Astra Linux Special Edition "Smolensk" (x64), versions:
  • 1.7[3]
  • 1.8
• Astra Linux Special Edition "Orel" (x64), versions:
  • 1.7[3]
  • 1.8
• Astra Linux Special Edition "Voronezh" (x64), versions:
  • 1.7[3]
  • 1.8
• RED OS, versions:
  • 7.3
  • 8.0
• ALT Linux OS, versions:
  • Workstation 10
  • Workstation 11.1[2]
  • Server 10.1 with the "Office server" profile
  • SP Server 10.1
• MOS 12.0
• macOS Sequoia, versions:
  • 15 (all builds)
• macOS Tahoe, versions:
	Supported kernel versions:
	Astra Linux Special Edition 1.7, editions "Orel", "Voronezh", and "Smolensk"
	• 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 from version 7.15.2)
	• 5.4.0-218-generic (starting from version 7.18.4)
	• 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 from version 7.15.2)
	• 5.10.233-1-generic (starting from version 7.17.2)
	• 5.10.239-1-generic (starting from version 7.18.4)
	• 5.10.241-1-generic (starting from version 7.19.2)
	• 5.10.248-1-generic (starting from version 7.19.4)
	• 5.10.254-1-generic (starting from version 7.21.6)
	• 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 from version 7.15.1)
	• 5.15.0-127-generic (starting from version 7.17.4)
	• 5.15.0-142-generic (starting from version 7.18.4)
	• 5.15.0-158-generic (starting from version 7.19.2)
	• 5.15.0-170-generic (starting from version 7.19.4)
	• 5.15.0-179-generic (starting from version 7.21.6)
	• 6.1.50-1-generic#astra2+ci6 (up to version 7.13.5)
	• 6.1.50-1-generic#astra4+ci68 (starting from version 7.13.6)
	• 6.1.90-1-generic (starting from version 7.15.1)
	• 6.1.124-1-generic (starting from version 7.17.2)
	• 6.1.141-1-generic (starting from version 7.18.4)
	• 6.1.152-1-generic (starting from version 7.19.2)
	• 6.1.161-1-generic (starting from version 7.19.4)
	• 6.1.170-1-generic (starting from version 7.21.6)
	Astra Linux Special Edition 1.7.10
	• 5.4.0-218-generic (starting from version 7.21.1 – 1.7.10.hotfix80)
	• 5.10.248-1-generic (starting from version 7.21.1 – 1.7.10.hotfix80)

Software	Additional requirements
• 26 (all builds) **Note:** [1] – Microsoft Windows 7 Service Pack 1 and Microsoft Windows Server 2008 R2 require the following Microsoft patches: KB4474419, KB4490628. The System checks for the presence of these patches on the computer before installing and/or updating the product. 2 – For all supported Linux family operating systems, interception via the X11 (X.Org) protocol is implemented. For OS ALT Workstation 11.1, interception via the Wayland protocol is also available. 3 – Starting with Device Monitor version 7.21.6, Astra Linux 1.7.11 cumulative update is supported.	• 5.15.0-170-generic (starting from version 7.21.1 – 1.7.10.hotfix80) • 6.1.161-1-generic (starting from version 7.21.1 – 1.7.10.hotfix80) Astra Linux Special Edition 1.8, editions "Orel", "Voronezh", and "Smolensk" • 6.1.90-1-generic (starting from version 7.17) • 6.1.124-1-generic (starting from version 7.17.5) • 6.1.141-1-generic (starting from version 7.17.10) • 6.1.152-1-generic (starting from version 7.18.8) • 6.1.158-1-generic (starting from 7.19.5) • 6.1.166-1-generic (starting from version 7.20.8) • 6.6.28-1-generic (starting from version 7.17) • 6.12.11-1-generic (starting from version 7.17.5) • 6.12.34-1-generic (starting from version 7.17.10) • 6.12.47-1-generic (starting from version 7.18.8) • 6.12.60-1-generic (starting from 7.19.5) • 6.12.77-1-generic (starting from version 7.20.8) Astra Linux Special Edition 1.8.6 • 6.1.166-1-generic (starting from version 7.21.2 – 1.8.6hotfix42) • 6.1.166-1-generic (starting from version 7.21.2 – 1.8.6hotfix44) • 6.1.166-1-generic (starting from version 7.21.4 – 1.8.6hotfix46) • 6.1.166-1-generic (starting from version 7.21.6 – 1.8.6hotfix49) • 6.12.77-1-generic (starting from version 7.21.2 – 1.8.6hotfix42) • 6.12.77-1-generic (starting from version 7.21.2 – 1.8.6hotfix44) • 6.12.77-1-generic (starting from version 7.21.4 – 1.8.6hotfix46) • 6.12.77-1-generic (starting from version 7.21.6 – 1.8.6hotfix49) Astra Linux Special Edition 1.8.7 • 6.1.177-1-generic (starting from version 7.21.7) • 6.12.95-1-generic (starting from version 7.21.7) • 6.18.38-1-generic (starting from version 7.21.7) RED OS 7.3 • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-4 • 5.15.35-5

Software	Additional requirements
	• 5.15.72-1 (starting from version 7.7.1) • 5.15.78-2 (starting from version 7.8) • 5.15.87-1 (starting from 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 from version 7.14.1) • 5.15.178-1 (starting from version 7.18.6) • 6.1.20-2 • 6.1.44-1 • 6.1.52-1 • 6.1.85-1 (starting from version 7.13.4) • 6.1.94-1 (starting from version 7.14.1) • 6.1.110-1 (starting from version 7.14.5) • 6.1.128-2 (starting from version 7.16.4) • 6.1.143-1 (starting from version 7.17.10) • 6.1.148-1 (starting from version 7.18.4) • 6.1.158-1 (starting from version 7.18.8) • 6.1.162-1 (starting from version 7.19.4) • 6.1.170-1 (starting from version 7.20.3) • 6.1.173-1 (starting from version 7.20.5) • 6.1.175-1 (starting from version 7.20.5) • 6.1.180-1 (starting from version 7.21.2) RED OS 8.0 • 6.6.6-1 (starting from version 7.17.0) • 6.6.26-1 (starting from version 7.17.0) • 6.6.34-1 (starting from version 7.17.0) • 6.6.51-1 (starting from version 7.17.0) • 6.6.76-1 (starting from version 7.17.0) • 6.12.21-1 (starting from version 7.17.3) • 6.12.37-1 (starting from version 7.17.10) • 6.12.56-1 (starting from version 7.18.8) • 6.12.69-1 (starting from version 7.19.4) • 6.12.85-1 (starting from version 7.20.3) • 6.12.90-1 (starting from version 7.20.5) • 6.12.92-1 (starting from version 7.20.5) • 6.12.101-1 (starting from version 7.21.2) 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 • 5.10.172-std-def-alt1

Software	Additional requirements
	• 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 from version 7.12.1) • 5.10.208-std-def-alt1 (starting from version 7.12.1) • 5.10.209-std-def-alt2 (starting from version 7.12.2) • 5.10.211-std-def-alt1 • 5.10.212-std-def-alt1 • 5.10.213-std-def-alt1 (starting from version 7.13.1) • 5.10.216-std-def-alt1 (starting from version 7.13.6) • 5.10.217-std-def-alt1 (starting from version 7.13.9) • 5.10.218-std-def-alt1 (starting from version 7.13.10) • 5.10.219-std-def-alt1 (starting from version 7.14.1) • 5.10.220-std-def-alt2 (starting from version 7.14.1) • 5.10.221-std-def-alt1 (starting from version 7.14.2) • 5.10.227-std-def-alt1 (starting from version 7.15.1) • 5.10.228-std-def-alt1 (starting from version 7.15.2) • 5.10.231-std-def-alt1 (starting from version 7.16.1) • 5.10.233-std-def-alt1 (starting from version 7.16.2) • 5.10.234-std-def-alt1 (starting from version 7.16.3) • 5.10.235-std-def-alt1 (starting from version 7.17.1) • 5.10.237-std-def-alt1 (starting from version 7.17.4) • 5.10.238-std-def-alt1 (starting from version 7.17.7) • 5.10.240-std-def-alt1 (starting from version 7.17.10) • 5.10.241-std-def-alt1 (starting from version 7.18.3) • 5.10.242-std-def-alt1 (starting from version 7.18.4) • 5.10.244-std-def-alt1 (starting from version 7.18.4) • 5.10.245-std-def-alt1 (starting from version 7.19) • 5.10.246-std-def-alt1 (starting from version 7.18.8) • 5.10.247-std-def-alt2 (starting from version 7.19.3) • 5.10.248-un-def-alt1 (starting from version 7.19.4) • 5.10.250-std-def-alt1 (starting from version 7.19.4) • 5.10.252-std-def-alt1 (starting from version 7.19.5)

Software	Additional requirements
	• 5.10.253-std-def-alt1 (starting from version 7.20.3) • 5.10.256-std-def-alt1 (starting from version 7.20.4) • 5.10.257-std-def-alt1 (starting from version 7.20.6) • 5.10.258-std-def-alt1 (starting from version 7.20.7) • 5.10.260-std-def-alt1 (starting from version 7.20.8) • 5.10.262-std-def-alt1 (starting from version 7.21.2) • 5.10.264-std-def-alt1 (starting from version 7.21.2) • 5.10.268-std-def-alt1 (starting from version 7.21.4) • 5.10.271-std-def-alt1 (starting from version 7.21.5) • 5.10.272-std-def-alt1 (starting from version 7.21.6) • 5.10.273-std-def-alt1 (starting from version 7.21.7) • 5.10.274-std-def-alt1 (starting from version 7.21.7) • 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 from version 7.13.2) • 6.1.67-un-def-alt0.c10f.1 (starting from version 7.12.4) • 6.1.75-un-def-alt1 (starting from version 7.12.2) • 6.1.77-un-def-alt1 (starting from version 7.12.2) • 6.1.78-un-def-alt1 (starting from version 7.12.4) • 6.1.79-un-def-alt1 (starting from version 7.12.5) • 6.1.80-un-def-alt1 • 6.1.81-un-def-alt1 • 6.1.82-un-def-alt1 (starting from version 7.13.1) • 6.1.83-un-def-alt1 (starting from version 7.13.2) • 6.1.84-un-def-alt1 (starting from version 7.13.4) • 6.1.85-un-def-alt1 (starting from version 7.13.4) • 6.1.90-un-def-alt1 (starting from version 7.13.8) • 6.1.94-un-def-alt1 (starting from version 7.14.1) • 6.1.96-un-def-alt1 (starting from version 7.14.1) • 6.1.99-un-def-alt1 (starting from version 7.14.2) • 6.1.112-un-def-alt1 (starting from version 7.15.0) • 6.1.113-un-def-alt1 (starting from version 7.15.1) • 6.1.115-un-def-alt1 (starting from version 7.15.2) • 6.1.119-un-def-alt1 (starting from version 7.16) • 6.1.121-un-def-alt1 (starting from version 7.16.1) • 6.1.123-un-def-alt1 (starting from version 7.16.1) • 6.1.124-un-def-alt1 (starting from version 7.16.2) • 6.1.127-un-def-alt1 (starting from version 7.16.3) • 6.1.128-un-def-alt1 (starting from version 7.16.3) • 6.1.129-un-def-alt1 (starting from version 7.16.4) • 6.1.130-un-def-alt1 (starting from version 7.17.1) • 6.1.131-un-def-alt1 (starting from version 7.17.1) • 6.1.132-un-def-alt1 (starting from version 7.17.2) • 6.1.140-un-def-alt1 (starting from version 7.17.4)

Software	Additional requirements
	• 6.1.141-un-def-alt1 (starting from version 7.17.7) • 6.1.144-un-def-alt1 (starting from version 7.17.10) • 6.1.146-un-def-alt1 (starting from version 7.17.10) • 6.1.147-un-def-alt1 (starting from version 7.18.1) • 6.1.148-un-def-alt1 (starting from version 7.18.3) • 6.1.151-un-def-alt1 (starting from version 7.18.4) • 6.1.153-un-def-alt1 (starting from version 7.18.4) • 6.1.157-un-def-alt1 (starting from version 7.18.6) • 6.1.158-un-def-alt1 (starting from version 7.18.8) • 6.1.159-un-def-alt1 (starting from version 7.19.2) • 6.1.159-un-def-alt1 (starting from version 7.19.2) • 6.1.160-un-def-alt1 (starting from version 7.19.4) • 6.1.161-un-def-alt1 (starting from version 7.19.4) • 6.1.163-un-def-alt1 (starting from version 7.19.4) • 6.1.166-un-def-alt1 (starting from version 7.19.5) • 6.1.167-un-def-alt1 (starting from version 7.19.7) • 6.1.168-un-def-alt1 (starting from version 7.19.7) • 6.1.169-un-def-alt1 (starting from version 7.20.3) • 6.1.173-un-def-alt1 (starting from version 7.20.4) • 6.1.174-un-def-alt1 (starting from version 7.20.6) • 6.1.175-un-def-alt1 (starting from version 7.20.7) • 6.1.177-un-def-alt1 (starting from version 7.20.8) • 6.1.180-un-def-alt1 (starting from version 7.21.2) • 6.1.182-un-def-alt1 (starting from version 7.21.2) • 6.1.186-un-def-alt1 (starting with version 7.21.4) ALT Workstation 11.1 • 6.12.41-6.12-alt1 • 6.12.59-6.12-alt1 • 6.12.74-6.12-alt1 • 6.12.85-6.12-alt1 (starting from version 7.20.3) • 6.12.94-6.12-alt1 (starting from version 7.20.7) • 6.12.96-6.12-alt1(starting from version 7.21.1) • 6.12.98-6.12-alt1 (starting from version 7.21.2) • 6.12.103-6.12-alt1 (starting from version 7.21.4) • 6.12.110-6.12-alt1 (starting from version 7.21.5) • 6.12.112-6.12-alt1 (starting from version 7.21.5) • 6.12.115-6.12-alt1 (starting from version 7.21.7) • 6.18.34-6.18-alt1 (starting from version 7.20.7) MOS 12.0 • 5.4.150-generic-1rosa2021.1 (starting from version 7.21.0) • 5.10.244-generic-1rosa2021.1 (starting from version 7.21.0) • 5.10.260-generic-1rosa2021.1 (starting from version 7.21.1) • 5.10.272-generic-1rosa2021.1 (starting from version 7.21.6)

Software	Additional requirements
	• 5.15.193-generic-2rosa2021.1 (starting from version 7.21.0) • 5.15.211-generic-1rosa2021.1 (starting from version 7.21.1) • 5.15.223-generic-1rosa2021.1 (starting from version 7.21.6) • 5.16.19-generic-2rosa2021.1 (starting from version 7.21.0) • 5.17.11-generic-2rosa2021.1 (starting from version 7.21.0) • 6.1.152-generic-2rosa2021.1 (starting from version 7.21.0) • 6.1.190-generic-1rosa2021.1 (starting from version 7.21.6) • 6.6.126-generic-1rosa2021.1 (starting from version 7.21.0) • 6.6.144-generic-1rosa2021.1 (starting from version 7.21.1) • 6.6.160-generic-1rosa2021.1 (starting from version 7.21.6) • 6.12.47-generic-5rosa2021.1 (starting from version 7.21.0) • 6.12.74-generic-2rosa2021.1 (starting from version 7.21.0) • 6.12.91-generic-6rosa2021.1 (starting from version 7.21.0) • 6.12.91-generic-10rosa2021.1 (starting from version 7.21.1) • 6.12.91-generic-19rosa2021.1 (starting from version 7.21.1) • 6.12.91-generic-20rosa2021.1 (starting from version 7.21.1) • 6.12.112-generic-8rosa2021.1 (starting from version 7.21.6) • 6.12.115-generic-8rosa2021.1 (starting from version 7.21.7) • 6.18.53-generic-1rosa2021.1 (starting from version 7.21.5) • 6.18.57-generic-3rosa2021.1 (starting from version 7.21.6) • 6.18.59-generic-1rosa2021.1 (starting from version 7.21.6)

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.

5 Installing InfoWatch Device Monitor

Installation is performed in the following order:

1. Preparing the environment.
2. Installing the Platform with the Investigation Centre.
3. Installing the Device Monitor server.
4. Configuring certificate verification for remote servers.
5. Obtaining the public key of the Platform.
6. Installing Device Monitor Agents.

5.1 Distribution kit contents

Device Monitor distribution kit is an archive named `dmsl_setup_X.X.X.xxx.tar.gz`, where `X.X.X` is the version number and `xxx` is the build number. The distribution kit includes the following components:

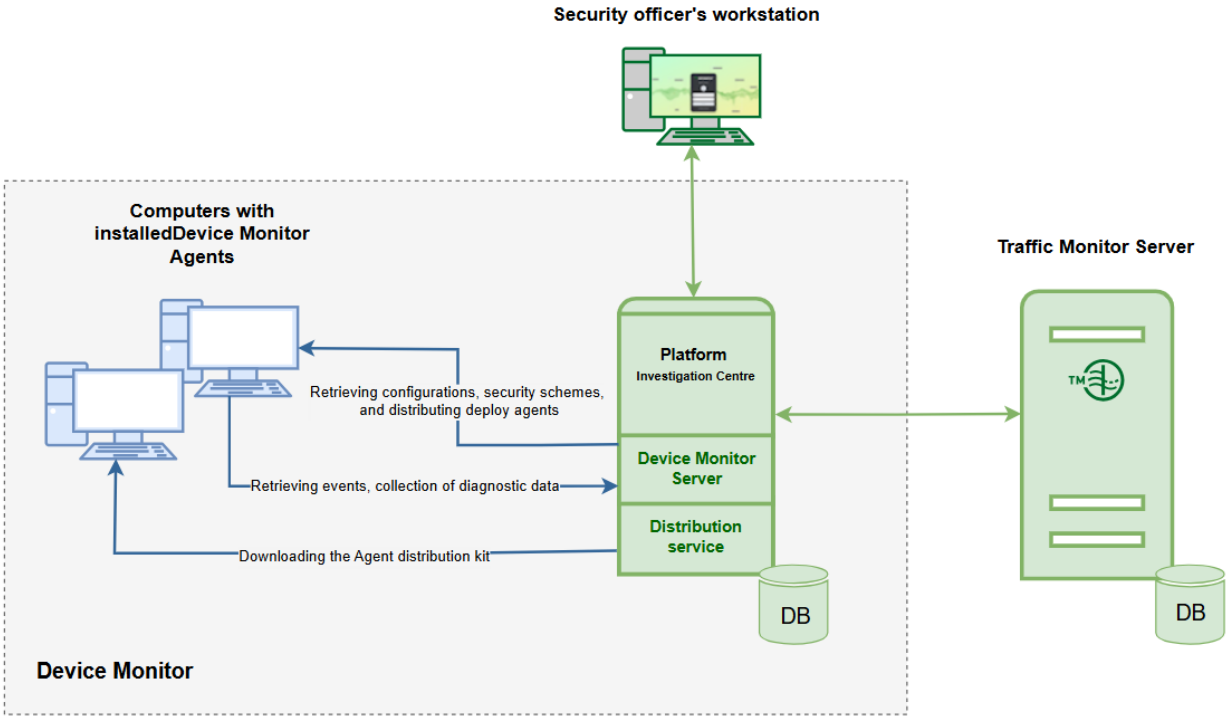
- `data/iwdms` – contains an archive with the Device Monitor Server executable files and a script for its installation with support for installation via command-line parameters;
- `data/scripts/include` – contains auxiliary scripts that are required for the proper operation of `setup.sh` and `install_iwdms.sh`;
- `data/ui` – Platform distribution kit with the web interface of the Investigation Centre;
- `setup.sh` – the script that launches the Device Monitor Server installer in the Linux terminal.

5.2 Deployment Scheme for Device Monitor

Find the InfoWatch Device Monitor components in the following table:

Component	Purpose
InfoWatch Device Monitor agent (Agent)	Collects data and monitors operations on workstations.
InfoWatch Device Monitor server (Server)	Distributes the security scheme to workstations with Agents, receives data from Agents and transmits it to the InfoWatch Traffic Monitor system, distributes the deploy agents to workstations.
InfoWatch Device Monitor database (Database)	Stores events and data that is required for the operation of Device Monitor.
Platform-based web interface	Manages the Device Monitor and Device Control modules.
Distribution service	Stores the new version of the distribution kit and delivers the Device Monitor Agent distribution kit to workstations.

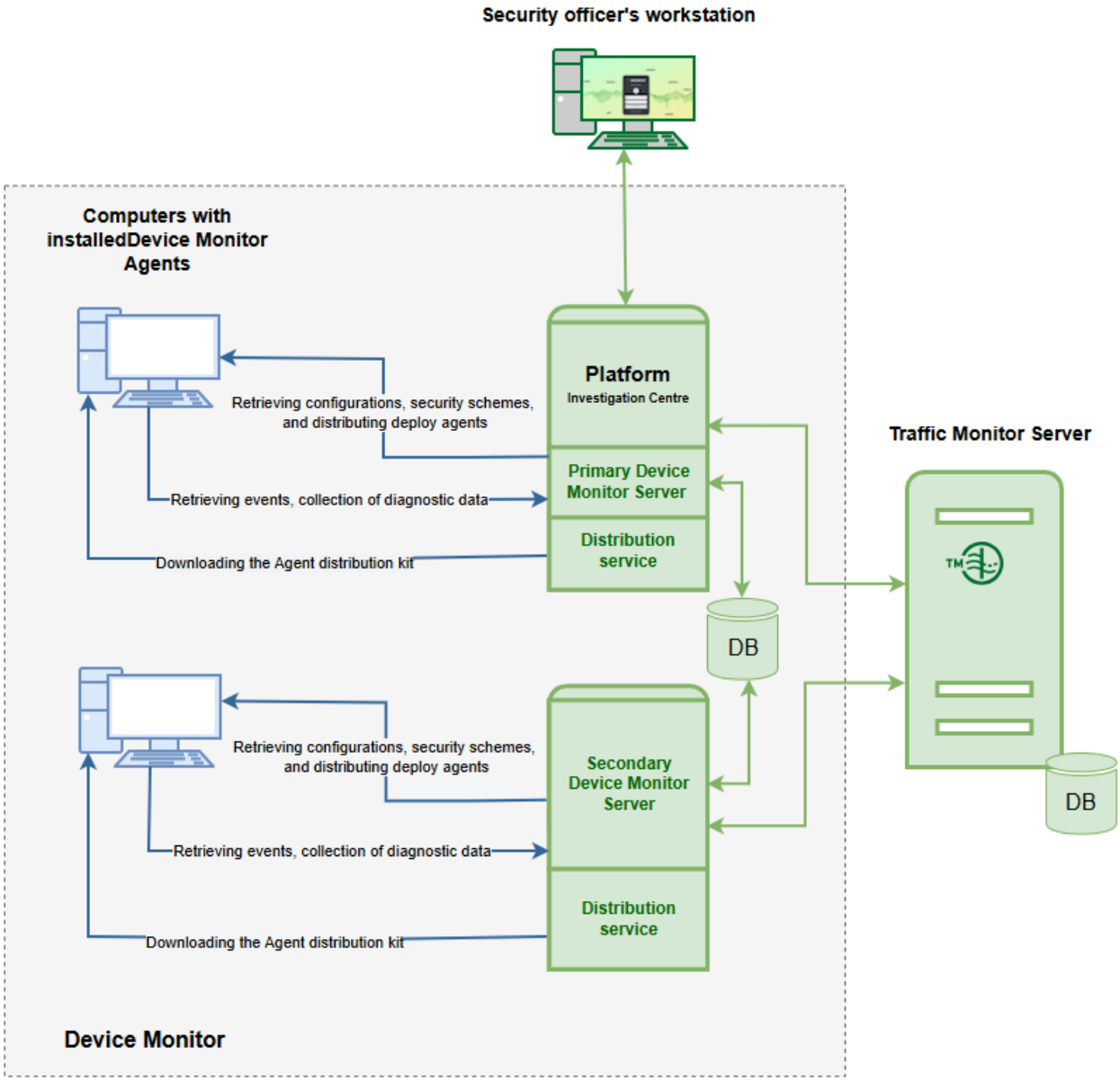
The Security officer connects to the Investigation Centre web interface from their workstation, where they can configure the security scheme and manage the Device Monitor and Device Control modules. The interaction of the Device Monitor components is shown in the figure:



To improve the productivity of Device Monitor, follow these recommendations:

- Use several Device Monitor servers. When you do so:
  - one Database scheme is used by several servers to store and distribute the overall security scheme;
  - the Agent checks the availability of all servers in the pool over the network and connects to one of the available servers.
- The Server and the Database can be located on the same computer. However, to improve performance, we recommend to place them on different computers.

Scheme with several Device Monitor servers:



System installation sequence:

1. Determine the scale of the system within the company's infrastructure and, with the help of the InfoWatch specialists, agree on the system requirements in accordance with this scale.
2. Determine the location and install the **Database**. It can be located either separately or on the same computer as the Device Monitor Server.
3. The basis for the Device Monitor installation is the Platform. The installer contains both the Platform and the product components. Both parts are mandatory for installation. First, install the central node of the **Platform**. It contains the web interface of the **Investigation Centre** for working with the products and the **Administration Centre** for configuring the Device Monitor Server. Here, you can configure the security scheme in accordance with the requirements of the corporate security policy and manage the Agents.
4. Install the **Device Monitor primary server** on the **Platform**. At the same time:

- specify the location of the **Databases**;
- install the **Distribution service**. The service has a repository with Agent distribution kits for supported operating systems.

Next, you can configure the security scheme in accordance with the requirements of the corporate security policy and manage the Agents.

- If you plan to use more than 500 Agents on workstations, install the **Device Monitor auxiliary servers**.
- Install the Agents on the workstations. You can do this either locally on the monitored workstation itself or remotely using the distribution task in the Investigation Centre web interface. In the second case, the **primary server** will distribute the Device Monitor deploy agents to the **workstations**, which will then download the Agent distribution kits from the nearest **distribution service** via the specified distribution publication points. The distribution downloads are carried out by several workstations simultaneously.

System operation sequence:

1. After the installation, the Agents connect to the Device Monitor server via a channel with traffic encryption based on an encryption key that is shared for the Agent and the Server.
2. The Agents receive the settings and the security scheme.
3. The Agents collect information about events that fall under the scope of the security scheme and policies, create shadow copies of files, and transmit this information to the Device Monitor server.
4. The server receives events and shadow copies and sends them to Traffic Monitor or Activity Monitor.

Example 1

An employee working on a controlled workstation begins a conversation in the VK messenger with an external person. At the same time, a rule is configured in Device Monitor that allows monitoring the exchange of chat messages and any types of outgoing files in the VK web version. Message exchange is tracked, and shadow copies of the transmitted files are sent for analysis to Traffic Monitor if the file size falls within the specified range.

Example 2

In Device Monitor, a rule has been defined that monitors the printing of text files. The rule states that when such an operation is performed, a shadow copy of the document should be created.

1. An employee working on a monitored workstation performs actions that result in the document being sent to print.
2. If the print job is successfully generated, the Device Monitor Agent generates an event and creates a shadow copy of the document sent to print.
3. If it is not possible to create a shadow copy of the document (for example, there is not enough free space on the hard drive), the print operation will be performed without creating a shadow copy, and this will be indicated in the event information.
4. The agent transmits the data (the event and the shadow copy of the document) to the Device Monitor Server. If there is no connection to the Server, the data is saved on the monitored computer. Once the connection is restored, the data will be sent to the Server.
5. The server sends the data to the
   This page has not yet been translated to English.
   system for analysis. If there is no connection to the InfoWatch Traffic Monitor server, the data is saved in the database. Once the connection is restored, the data will be sent to the InfoWatch Traffic Monitor system.

5.3 Preparing the Environment

To ensure the Device Monitor Server operation, you need to prepare the environment:

1. Enter the computer where the Device Monitor Server will be installed into the domain.
2. Make sure that the server has an FQDN hostname configured. To do this, run the command:

   ```
   echo $HOSTNAME
   ```

   As a result, the full name should be displayed, such as `dmserv.company.ru`

   If a short name is displayed, such as dmserv, then:

   a. Set the full name of the host:
      - On a computer running Astra Linux, ALT OS, or Mos.OS, use the command:

```
hostnamectl set-hostname <FQDN>
```

- On a computer running RED OS:
  1. Run the `nmtui` utility:

     ```
     nmtui
     ```

  2. In the text interface, select `Set system hostname`.
  3. In the `Set Hostname` window, enter the new hostname and click `OK`.
  4. In the `Set hostname to '<new_name>'` window, click `OK`.
  5. Click `Quit`.

b. Restart the server.

c. Run the command again:

```
echo $HOSTNAME
```

3. Install Microsoft .NET 8 (https://dotnet.microsoft.com/) on this computer. See the installation examples below.

   Note:

   If you plan to install the Device Monitor Server with containerization support (see New Installation), then installing .NET 8 is not required.

4. Complete the Inotify subsystem settings. For this:

   a. Open the configuration file `/etc/sysctl.conf` for editing.

   b. Add the following strings at the end of the file:

   ```
   fs.inotify.max_user_instances = 16384
   fs.inotify.max_user_watches = 32768
   fs.inotify.max_queued_events = 262144
   ```

   You can also set the maximum number of files to be opened. To do this, specify the value of the `file-max` parameter, such as:

   ```
   fs.file-max = 500000
   ```

   c. Save the changes and close the configuration file.

   d. To apply the new subsystem settings, run the command:

   ```
   sysctl -p
   ```

5. If the installation is performed on a server running Mos.OS, make sure that the official OS repositories are available: `software`, `update`, `oss-suse`.
6. Install the `conntrack` (or `conntrack-tools`) and `socat` packages. For an example of package installation, see below.
7. If you are going to use the option to install the server with containerization support, install the `podman` package.

   Examples for installing the podman package on ALT OS, Astra Linux, RED OS, and Mos.OS:

   - **ALT OS**:

   ```
   apt-get install podman
   ```

- **Astra Linux**:

```
apt install podman
```

- **RED OS**:

```
sudo dnf install podman
```

If the package is not available in the repository, download it from the official RED OS website. Go to the directory with the package and install it manually using a command like:

```
rpm -Uhv ./<package_name>
```

> **Important!**
>
> The minimum version of `podman` for RED OS 4.9 is required.
>
> If you install the `podman` package on RED OS manually, also install the dependent packages required for its operation.

- **Mos.OS**:

```
zypper install podman
```

8. Configure the antivirus for joint operation with the System (see Antivirus configuration for Device Monitor Server on Linux OS).
9. Configure the POD network rules or disable the firewall (see Firewalld and Kubernetes interaction conflicts, Firewall complete shutdown).
10. Install the Python version 3 interpreter. The package with the interpreter is not included in the product distribution kit.
11. **If the installation is performed on a server running RedOS, Mos.OS, or Astra Linux:**
Install the following packages:
    - **RED OS**:

```
dnf install python3-pyyaml
dnf install python3-importlib-metadata
```

    - **Astra Linux**:

```
apt-get install python3-importlib-metadata
apt-get install python3-distutils
apt-get install python3-mako
apt-get install python3-yaml
```

    - **Mos.OS**:

```
zypper install python3-PyYAML
zypper install python3-importlib-metadata
```

> **Note:**
>
> The packages may be missing in the product distribution kit and repositories. In this case, download and install the required packages manually.

12. **If the installation is performed on a server running ALT OS:**
    - Install the `unzip` utility in the same way as you installed `conntrack` and `socat`.
    - Install the following packages:

```
apt-get install python-modules-json
apt-get install python-modules-distutils
apt-get install python3-modules-sqlite3
apt-get install python3-module-yaml
apt-get install python3-module-importlib-metadata
```

Note:

The packages may be missing in the product distribution kit and repositories. In this case, download and install the required packages manually.

- Configure the correspondence between the encryption algorithms of the Device Monitor and Traffic Monitor Servers. To do this, modify the file `/etc/openssl/openssl.cnf` as follows:
  - Find the strings in the file:

```
# Extra OBJECT IDENTIFIER info:
#oid_file       = $ENV::HOME/.oid
oid_section     = new_oids
```

  - After them, add the strings:

```
# System default
openssl_conf = default_conf
```

  - Add the following strings to the end of the file:

```
[default_conf]
ssl_conf = ssl_sect

[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString =  DEFAULT:@SECLEVEL=1
```

13. **If the installation is performed using the Host option on a server running Astra Linux 1.8:**
    - Configure the correspondence between the encryption algorithms of the Device Monitor and Traffic Monitor Servers. To do this, modify the file `/etc/openssl/openssl.cnf` as follows:
      - Find the strings in the file:

```
# Extra OBJECT IDENTIFIER info:
#oid_file       = $ENV::HOME/.oid
oid_section     = new_oids
```

      - After them, add the strings:

```
# System default
openssl_conf = default_conf
```

      - Add the following strings to the end of the file:

```
[default_conf]
```

```
ssl_conf = ssl_sect

[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString =  DEFAULT:@SECLEVEL=1
```

14. **If the installation is performed using the Host option on a server running RED OS 8:**
    Install the package `openldap-compat`:

    ```
    dnf install openldap-compat
    ```

    If you installed the package after installing the Device Monitor server, restart the `webapi` service:

    ```
    systemctl restart iwdms_webapi
    ```

15. **If the installation is performed on a server running Mos.OS:**
    Install the packages `ethtool`, `app_armor`, `fuse-overlayfs,` and `sysctl` with dependencies:

    ```
    zypper install ethtool
    zypper install patterns-base-apparmor
    zypper install procps
    zypper install fuse-overlayfs
    ```

16. **If you plan to distribute Agents to workstations running Windows OS:**
    Install the Samba client on the server:
    - **RED OS**:

      ```
      dnf install samba samba-client samba-common-tools
      ```

    - **Astra Linux**:

      ```
      apt install samba samba-common smbclient
      ```

      In the case of a server running Astra Linux 1.7 and the installation of the Samba client from the local repository, the `smbclient` and `samba-common` packages must be version 4.19.6 or later.
    - **ALT OS**:

      ```
      apt-get install samba samba-client smbclient
      ```

    > **Note:**
    > If you plan to install the Device Monitor Server with containerization support (see New Installation), then installing the Samba client on the server is not required.

17. Install the PostgreSQL DBMS.
    We recommend to install the DBMS on another computer. If you need to receive events from a small number of Agents, you can install the PostgreSQL DBMS together with the Device Monitor Server.
    Example of installing PostgreSQL 15 on RED OS
    a. Update the packages installed in the system:

```
sudo dnf update
```

b. Install and initialize the DBMS by running the following commands:

```
sudo dnf install postgresql
sudo dnf install postgresql15-server
sudo postgresql-15-setup initdb
sudo systemctl enable postgresql-15.service --now
```

c. Make sure the PostgreSQL service is running and has the status **`active`**:

```
sudo systemctl status postgresql-15.service
```

You can also obtain information on installing PostgreSQL on RED OS from the official RED OS documentation.

> **Note:**
>
> To ensure the correct and uninterrupted operation of the Server, store the DBMS files and shadow copies of events on different physical disks. To work with the DBMS, you need a role with the rights to create a database.

18. Additionally configure the database.

> **Important!**
>
> The file names `postgresql.conf` and `pg_hba.conf` are the same for all operating systems, but paths to them differ. The article provides example paths used on RED OS.

a. Open the file `/var/lib/pgsql/15/data/`**`postgresql.conf`**.

b. Enable the ability to escape special characters when inserting strings into database tables. To do this, set the `"standard_conforming_strings"` parameter to `on`.

c. Set the parameters that optimize performance. For a more precise selection of parameters, use the PGTune calculator.

   i. Assign the value 250 to the `"max_connections"` parameter.

   ii. Configure the log rotation.

   iii. Specify other parameters (memory resource consumption, WAL settings, query planning) in accordance with the official PostgreSQL documentation.

d. If you are going to use the option to install a server with containerization support and place the database on a single server with Device Monitor:
Find the string in the file:

```
# listen_addresses = 'localhost'
```

and replace it with the following:

```
listen_addresses = '*'
```

e. Open the `/var/lib/pgsql/15/data/`**`pg_hba.conf`** file for editing.

f. If you are going to use the option to install a server with containerization support and place the database on a single server with Device Monitor, add the following parameter as the first line:

```
host all all 0.0.0.0/0 md5
```

g. If you are installing the DBMS on a server that is separate from Device Monitor, configure access to the DBMS in the `pg_hba.conf` file in accordance with the official PostgreSQL documentation.
h. Restart the PostgreSQL service.
Example command for RED OS:

```
sudo systemctl restart postgresql-15.service
```

i. If you plan to subsequently install the System with containerization support and use Oracle Linux, we recommend you to install the language pack after installing the DBMS:

```
sudo dnf install langpacks-ru -y
```

19. Configure the password for `postgres`. For this:
    a. Log in as a `postgres` user:

    ```
    su - postgres
    ```

    b. Run the program `psql`:

    ```
    psql
    ```

    c. Enter the password setting command:

    ```
    \password postgres
    ```

    d. Enter the new password twice.
    e. Log out of the `psql` program and switch the `postgres` user:

    ```
    \q
    exit
    ```

20. To successfully connect the Device Monitor Server to the Traffic Monitor Server, configure the remote server certificate verification (see Configuring Validation of the Remote Server Certificates). You can also do this after the installation.
21. **If you plan to use the Kerberos protocol to retrieve information about employees and computers from MS Active Directory:**
    - If Device Monitor is installed using the *Host* option:
        i. Make sure that the Device Monitor Server time matches the domain controller time. The maximum allowable deviation is 5 minutes. If necessary, install and configure `chrony` or `ntpd`.
        ii. Make sure that the file `/etc/resolv.conf`:
            - has the search domain properly specified;
            - Active Directory DNS servers are specified as DNS servers.
        iii. Install the packages `krb5-workstation`, `krb5-libs`, `cyrus-sasl-gssapi`. You can also install the package `openldap-clients` for diagnostics in case of connection errors.
        iv. Configure the Kerberos protocol configuration file `/etc/krb5.conf`. Make sure to respect the case when specifying Realm addresses.
    - When installing Device Monitor using the *Container* option:

i. Install the `openldap-clients` package to diagnose connection errors.

ii. Configure the Kerberos protocol configuration file `/opt/iw/dmserver/etc/krb5.conf`. Make sure to use the correct case when specifying Realm addresses.

- Fill in the `default_ccache_name` parameter as follows:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

> **Note:**
> The steps can also be performed after installing the Device Monitor Server.

22. Make sure that the server has the current date and time set.

5.3.1 Examples of installing additional packages

Example of installing .NET on ALT OS

1. Make sure that the ALT OS repositories are available by running the command:

```
apt-repo list
```

2. If the repositories are unavailable (commented out), you need to edit the `/etc/apt/sources.list` file by uncommenting the strings containing the repository addresses.
3. Edit the file `/etc/apt/apt.conf`:
   a. Uncomment all stings.
   b. Provide the correct username and password for the domain account.
4. Install the .NET 8 runtime with the necessary ASP.NET Core support. To do this, run the command in the terminal:

```
apt-get install dotnet-aspnetcore-runtime-8.0
```

As a result, the .NET 8 runtime environment with ASP.NET Core support will be installed.

5. Check the installed .NET 8 by running the command:

```
dotnet --info
```

```
[root@altserver ~]# dotnet --info

Host:
  Version:      8.0.11
  Architecture: x64
  Commit:       8.0.11-alt
  RID:          linux-x64

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 8.0.11 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 8.0.11 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]
```

Example of installing .NET on Astra Linux

1. Make sure that the Astra Linux repositories are available by running the command:

```
apt-get update
```

2. If the repositories are unavailable (commented out), you need to edit the `/etc/apt/sources.list` file by uncommenting the lines containing the repository addresses.
3. Edit the file `/etc/apt/apt.conf`:
    a. Uncomment all strings.
    b. Provide the correct username and password for the domain account.
4. Install the .NET 8 runtime with the necessary ASP.NET Core support. To do this, run the following command in the terminal:

```
apt install aspnetcore-runtime-8.0
```

As a result, the .NET 8 runtime environment with ASP.NET Core support will be installed.

> **Note:**
>
> The packages required to install .NET 8 may be missing in the repositories. In this case, download and install the required packages manually.
> For more information about installing .NET on Astra Linux, see the official websites: Astra Linux: Installing MS .Net Core and MS Visual Studio Code and .Net.

5. Check the installed .NET 8 by running the command:

```
dotnet --info
```

```
root@astra-smolensk-1-8:~# dotnet --info

Host:
  Version:      8.0.0
  Architecture: x64
  Commit:       5535e31a71
  RID:          debian.12-x64

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 8.0.0 [/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 8.0.0 [/usr/share/dotnet/shared/Microsoft.NETCore.App]
```

Example of installing .NET on Astra Linux

1. Make sure that the RED OS repositories are available by running the command:

```
dnf repoinfo
```

2. Install the .NET 8 runtime with the necessary ASP.NET Core support. To do this, run the following command in the terminal:

```
sudo dnf install aspnetcore-runtime-8.0
```

In some Linux distributions, the package name may be `dotnet-aspnetcore-runtime-8.0`
As a result, the .NET 8 runtime environment with ASP.NET Core support will be installed.

3. Check the installed .NET 8 by running the command:

```
dotnet --info
```

```
[root@[redacted] ~]# dotnet --info

Host:
  Version:      8.0.17
  Architecture: x64
  Commit:       77545d6fd5
  RID:          redos.7.3-x64

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.35 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.AspNetCore.App 8.0.17 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.35 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]
  Microsoft.NETCore.App 8.0.17 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]
```

If errors occur during the installation of .NET:

- Remove all packages related to .NET from the operating system. Run the command:

```
sudo dnf remove 'dotnet*' 'aspnet*' 'netstandard*'
```

- Reinstall a specific version of .NET, for example:

```
sudo dnf install aspnetcore-runtime-8.0-8.0.17-1.el7
```

- To view the list of available versions, run:

```
dnf --showduplicates list aspnetcore-runtime-8.0
```

Example of installing `conntrack and socat` on RED OS

To ensure proper Kubernetes support, check that the `conntrack` and `socat` packages are installed.

For this:

1. In the command line, type:

```
conntrack
```

   In response, you will see information about the operation and the current version of this package.

2. If `conntrack` is not installed, install it using the command:

```
sudo dnf install conntrack
```

3. If the package is not available in the repository, download it, navigate to the directory containing the package, and install it manually using a command like:

```
rpm -Uhv ./<package_name>
```

4. Repeat the steps described above to install the `socat` package.

5.4 New Installation

Possible Device Monitor installation options:

- **All-in-one** option involves hosting the Device Monitor Server and the Platform with the web interface of the Investigation Centre and the Administration Centre on a single server.
- **Distributed** installation of the Device Monitor Server on the office node of the Platform.

> **Important!**
>
> When using a distributed installation, take into account the following key aspects:

- Products in the cluster must be installed on the same version of the Platform. If you install a product in the cluster on a new version of the Platform, you will need to update all products for them to work correctly.
- In a single cluster, you can deploy only one central node of the Platform, and each product in central mode can exist in only one instance.
- If a product is already installed in the cluster in `central` mode, another installation of this product in the `central` mode in the same cluster will fail with an error.
- Device Monitor supports installation only in the `central` mode. At the same time, it supports installation on both the central and office nodes of the Platform.

Products in the same cluster have:

- access to all functionality in the Investigation Centre interface, which is the same for all products;
- common settings;
- common role model;
- shared access to data regardless of which product is integrated with the source, as well as access to processed data.

Important!

When migrating from Windows to Device Monitor for Linux, you can save the data, meaning you can continue using the same database that was used with the server of Device Monitor for Windows. During the migration, the structure and contents of the database are automatically modified. To ensure correct migration:

- Make sure that the database is ready for migration; otherwise, prepare it. For details, see Preparing the Device Monitor Server for Migration from Windows to Linux-based Operating Systems.
- During the installation, at the step where you configure the interaction with the database, select **Update an existing database**.
- After installation, make sure that Russian locale is set for the database (`ru_RU.utf8`). For details, see Checking and changing the PostgreSQL database locale.

5.4.1 "All-in-one" installation mode

This mode is suitable for installing the web interface, the Device Monitor Server, and the database on a single server, as well as when transitioning to Device Monitor for Linux from Windows.
To install Device Monitor in "All-in-one" mode:

1. Make sure the server meets the hardware and software requirements (see Hardware and Software Requirements).
2. Follow the steps to prepare the server for Device Monitor installation (see Preparing the Environment).
3. Copy the archive containing the Device Monitor Server distribution kit to the hard drive.
4. Create a directory and unpack the contents of the archive into it. In the example, the archive will be unpacked into the `/dmsl_distr` directory:

```
mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.0.310.tar.gz -C /dmsl_distr
```

5. Go to the created directory.
6. Run the **setup.sh** script, which is included in the distribution kit:

```
./setup.sh
```

> **Note:**
>
> If you encounter a permission error when running the script, make the file executable using the command:
>
> ```
> chmod +x ./setup.sh
> ```
>
> Then run the script.

After that, the following actions will be available:

- **Install** – new installation;
- **Update** – updating installed components;
- **Utilities** – going to the utilities menu;
- **Exit** – exiting the program.

7. Select the installation type **Install**. A list of components will be available:
   - **DM Server Service, Front End** – "All-in-one" installation, meaning the installation of the Device Monitor Server and the Front End component;

     > **Note:**
     >
     > The Front End component is required for the work of the Administration Centre and needs to be installed even if another Platform-based product is already installed on the server.

   - **Front End only** – installation of the Platform and the web interface only;
   - **DM Server Service only** – installation of the Device Monitor Server only.
8. For "All-in-one" installation, select **DM Server Service, Front End**.
9. Select the Device Monitor server installation option:
   - **Host**, to install the server on a host; or
   - **Container (podman)**, to install the server with containerisation support.
10. Installation modes for the Platform with the web interface of the Investigation Centre and the Administration Centre will be proposed to you:
    - **Central** – intended for installation on the primary node or if there is no already installed web interface;
    - **Office** – intended for distributed installation.
11. Select the mode **Central**.
12. View the terms of the license agreement. It contains several pages. To go to the next page, press **Enter**.
13. Type **"y"** to accept the license agreement and press **Enter**.
14. Enter the IP-address of the server in the IPv4 format: `"xxx.xxx.xxx.xxx"` and press **Enter**.
15. Allocate RAM to host ClickHouse data (by default, 80%) and press **Enter**.
16. Specify the path to place ClickHouse data (by default: `/opt/chdata`) and press **Enter**.
17. Specify the path to place PostgreSQL data (by default: `/opt/pgdata`) and press **Enter**.
18. Specify the path to place NATS data (by default: `/opt/natsdata`) and press **Enter**.
19. Specify the path to place data (by default: `/opt/dsdata`) and press **Enter**.
20. Specify the path to temporarily place Traffic Monitor events before loading them to the Platform (by default: `/opt/factsldrtmdata`) and press **Enter**.
21. Specify the port for connecting to the web interface (by default, `443`) and press **Enter**.
22. Wait for the Platform installation to complete. The Device Monitor Server will be installed next. At the same time:
    a. Folders will be created:
       - `/var/log/iwdms` – folder for the Device Monitor server execution logs;
       - `/opt/iw/dmserver/bin` – folder with the Device Monitor server files;

- `/opt/iw/dmserver/queue` – file queue folder;
- `/opt/iw/dmserver/log` – symbolic link to the folder `/var/log/iwdms`

b. **iwdms** user with the key `--system` will be added, making it possible to run the service under this user, but not allowing to log in as this user in the Investigation Centre.
c. A ZIP file from `data/iwdms` of the installation package will be unpacked into the required folders. The **iwdms** user will be assigned as an owner for the aforementioned folders.
d. In the systemd folder of the services `/etc/systemd/system`, the file of the manifest of the Device Monitor Server service **iwdms.service** will be added, as well as services for syncing with Active Directory – **iwdms_ldap.service**.

23. Select the language of the server being installed and press **Enter**. This will determine the names of the preinstalled groups, policies, and rules.
24. Read the license agreement and select the required action. To continue the installation, you need to accept the license agreement. Select **Accept and continue** and press **Enter**.
25. Select the type of server you need to install: **Primary** or **Secondary**.
If you are installing the System for the first time or switch from Device Monitor that is installed on Windows, select **Primary**.
26. Configure interaction with the database:
    - **Create a new database** – to create a new database. Use this option for a **clean installation**;
    - **Update an existing database** – to configure the existing database. Use this option to **install with data migration**.
27. Specify the name or the IP address of the server where the PostgreSQL DBMS is located. If you are installing Device Monitor with data migration, use the PostgreSQL DBMS that was used to install the Device Monitor Server on Windows.
If you previously selected the installation option **Container (podman)** and placed the database on the same server with Device Monitor, then enter the address of the network interface of this server. Before this, configure the database (see Preparing the Environment).

> **Important!**
>
> If you selected the installation option **Container (podman)**, you cannot enter `localhost` or `127.0.0.1` as an IP address.

28. Specify the port for configuring interaction. If you do not specify it, the default `5432` port will be used.
29. Enter the name of the database. By default – `iwdm`.
30. Enter the name of the DBMS user. By default – `postgres`.
31. Enter the password.
32. Select **Yes** to install the distribution service. In this case, the distribution point will be able to spread the agent distribution kits to workstations. If you previously selected the **Container (podman)** server installation option, then the distribution service will also be installed with the containerisation support.
33. If you previously selected the **Primary** server, then specify the path to the PFX file of the key that encrypts the channel between the Device Monitor Server and the agents. If you do not specify the path, then the default `/opt/iw/dmserver/ssl.pfx` path will be used.
34. If you are installing the Server to the new database, then you need to create the encryption key. Select **Yes**.
35. Next, you can select the deployment type:
    a. **Interact with Traffic Monitor** – with the option to send events to Traffic Monitor;
    b. **Operate autonomously** – autonomous work without integration with Traffic Monitor.

Important!

When selecting the autonomous work mode, no predefined rules will be created in the policies by default.

Note:

After the installation, you can switch the autonomous mode in the section **Settings** → **Device Monitor servers**.

36. If you selected **Interact with Traffic Monitor** on the previous step, then enter the name of the server or its IP address.

Important!

The server name may contain Latin letters from "a" to "z" (case-insensitive), numbers from "0" to "9", and the hyphen "-". It cannot consist of numbers only. We recommend using the server name that starts with a letter.

Note:

If you need to change the InfoWatch Traffic Monitor address after the installation, you can do it in the Device Monitor server database:

- the field `TRAFFIC_MONITOR_POLICY_SERVER_ADDRESS` of the table Settings contains the address of the Traffic Monitor server that is used by all servers of the Device Monitor pool (both primary and secondary) to obtain the Traffic Monitor policy and distribute it to the agents;
- the `TmAddress` field in the ServerOption table contains the address of the Traffic Monitor server to which events from Device Monitor are sent. In this table, the `TmAddress` field may appear multiple times (depending on the number of servers in the pool).

37. If an access token to Traffic Monitor is requested, enter its value.
To successfully connect the Device Monitor Server with the Traffic Monitor Server, you need to configure the remote server certificate validation (see Configuring Validation of the Remote Server Certificates).
38. If you selected **Update an existing database**, a check if there are rules that do not support configuration in the new version of Device Monitor is launched. If unsupported rules are detected, the migration will fail. In this case, we recommend contacting the InfoWatch technical support.
39. If you selected **Update an existing database** and plan to use the Device Control module, rules, and white lists, select **Using Device Control is required, migrate rules and white lists**. Wait until the Device Control rules and white lists are migrated to the new version. If you do not plan to use Device Control, select **Using Device Control is not required, delete rules and white lists**.
40. Enter the IP address of the Device Monitor server.
41. During the initial installation of the Device Monitor Server and the database, you can load a custom configuration file with default policies and settings. To load the file, enter the path to it, such as `/root/configuration.zip`. In this case, all existing settings and configuration elements will be replaced with the imported ones.
To skip this step, press **Enter**.

Important!

The configuration file needs to be placed on a local disk or external storage device. Loading the file from a network folder is not supported.

42. Wait for the installation to complete.
If you are installing in "All-in-one" mode and have previously selected the **DM Server Service**, **Front End** option, the following actions will be performed automatically:

- the public key of the **guard** service of the Platform will be obtained and recorded in Device Monitor. The key is required for the correct interaction between the web interface and the Server;
- the **n.yaml** file will be corrected.

> **Important!**
>
> Any product that will be installed in the Investigation Centre after Device Monitor will generate a new **n.yaml** file, and the section that is necessary for the correct interaction of the web interface with the Server will be deleted from it. To restore **n.yaml**, follow the steps 43a–43d.

43. If you install the web interface on the Platform basis and the Device Monitor Server in sequence, using the **Front End only** and **DM Server Service only** installation options, the actions involving the Platform's **guard** service key and the **n.yaml** file from the previous step will not be performed automatically. After installing the Platform and the Server, perform them using the installer. To do this:
    a. Run the installation script:
    ```
    ./setup.sh
    ```
    b. Select **Utilities** from the menu. The section contains utilities:
        i. **Fix n.yaml file** – the utility for automatically adding the required settings to **n.yaml**. Select this option if the Platform with the web interface of the Investigation Centre and the primary Device Monitor server are installed on the current computer. You also need to perform this action after installing any product in the Investigation Centre;
        ii. **Save platform guard public key to IWDM Service** – if Device Monitor is installed on the current computer as the **primary** server, and the Platform is also installed (in either the central or office mode), then, by running this utility, you can automatically get the public key of the **guard** service of the Platform and save it to the server directory;
        iii. **Show IWDM Service version** – the utility displays the version of the installed server;
        iv. **Export ssl key** – the utility allows you to export the agent-server channel protection key.
    c. Select **Fix n.yaml file**.
    d. Enter the IP address of the Device Monitor server and wait for the process to complete.
    e. Run the installation script:
    ```
    ./setup.sh
    ```
    f. Select **Utilities** from the menu and then **Save platform guard public key to IWDM Service**. Wait for the process to complete.
    g. Restart the **iwdms** service:
    ```
    systemctl restart iwdms
    ```

> **Important!**
>
> To connect to the Investigation Centre web interface, **always** use the address or name of the server where the **Platform is installed in the** `central` **mode**.

5.4.2 Distributed installation of Device Monitor

A distributed installation is required when an organization also uses other InfoWatch products and/or has a structure with a central office and branches. In this case, you can install one or more Device Monitor Servers on computers with the Platform office nodes, where other InfoWatch products may also be installed.

To install the primary Device Monitor server in the distributed mode:

1. Make sure the server meets the hardware and software requirements (see Hardware and Software Requirements).
2. Follow the steps to prepare the server for the Device Monitor installation (see Preparing the Environment).
3. Copy the archive containing the Device Monitor Server distribution kit to the hard drive of another computer.
4. Create a directory and unpack the contents of the archive into it. In the example, the archive will be unpacked into the `/dmsl_distr` directory:

   ```
   mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.0.310.tar.gz -C /dmsl_distr
   ```

5. Go to the created directory.
6. Run the **setup.sh** script, which is included in the distribution kit:

   ```
   ./setup.sh
   ```

   Note:

   If you encounter a permission error when running the script, make the file executable using the command:

   ```
   chmod +x ./setup.sh
   ```

   Then run the script.
7. Select the installation type **Install**. A list of components will be available:
   - **DM Server Service, Front End** – "All-in-one" installation, that is installing the Device Monitor Server and the Front End component;

     Note:

     The Front End component is required for the work of the Administration Centre and needs to be installed even if another Platform-based product is already installed on the server.
   - **Front End only** – installing only the Platform and the web interface;
   - **DM Server Service only** – installing only the Device Monitor Server.
8. Select **DM Server Service, Front End**.
9. Select the Device Monitor server installation option:
   - **Host**, to install the server on the host; or
   - **Container (podman)**, to install a server with containerization support.
10. Installation modes for the Platform with a web interface of the Investigation Centre and the Administration Centre will be provided:
    - **Central** – intended for installation on the primary node or in the absence of an already installed web interface;
    - **Office** – intended for distributed installation.
11. Select the **Office** mode.
12. View the terms of the license agreement. It contains several pages. To go to the next page, press **Enter**.
13. Type **"y"** to accept the license agreement and press **Enter**.
14. Enter the IP address of the central node of the Platform that was installed earlier.
15. Get the token for the central node. To do this, run the following command on the server with the central node:

    ```
    kubeadm token list
    ```

16. Copy the received token.
17. Enter the token on the Platform office node and press **Enter**.
18. Specify the label for the Platform office node.
19. Allocate RAM to host ClickHouse data (by default, 80%) and press **Enter**.
20. Specify the path to place ClickHouse data (by default: `/opt/chdata`) and press **Enter**.
21. Specify the path to place PostgreSQL data (by default: `/opt/pgdata`) and press **Enter**.
22. Specify the path to place NATS data (by default: `/opt/natsdata`) and press **Enter**.
23. Specify the path to place data (by default: `/opt/dsdata`) and press **Enter**.
24. Specify the path to temporarily place Traffic Monitor events before loading them to the Platform (by default: `/opt/factsldrtmdata`) and press **Enter**.
25. Wait for the installation of the office node of the Platform to complete. Next, the Device Monitor Server will be installed. At the same time:
    a. Folders will be created:
        - `/var/log/iwdms` – folder for the Device Monitor server execution logs;
        - `/opt/iw/dmserver/bin` – folder with the Device Monitor server files;
        - `/opt/iw/dmserver/queue` – file queue folder;
        - `/opt/iw/dmserver/log` – symbolic link to the folder `/var/log/iwdms`
    b. **iwdms** user with the key `--system` will be added, making it possible to run the service under this user, but not allowing to log in as this user in the Investigation Centre.
    c. A ZIP file from `data/iwdms` of the installation package will be unpacked into the required folders. The **iwdms** user will be assigned as an owner for the aforementioned folders.
    d. In the systemd folder of the services `/etc/systemd/system`, the file of the manifest of the Device Monitor Server service **iwdms.service** will be added, as well as services for syncing with Active Directory – **iwdms_ldap.service**.
26. Select the language of the server being installed and press **Enter**. This will determine the names of the preinstalled groups, policies, and rules.
27. Read the license agreement and select the required action. To continue the installation, you need to accept the license agreement. Select **Accept and continue** and press **Enter**.
28. Select the **Primary** server type to install.
29. Configure the interaction with the database:
    - **Create a new database** – to create a new database. Use this option for a **clean installation**;
    - **Update an existing database** – to configure the existing database. Use this option to **install with data migration**.
30. Specify the name or the IP address of the server where the PostgreSQL DBMS is located. If you are installing Device Monitor with data migration, use the PostgreSQL DBMS that was used to install the Device Monitor Server on Windows.
    If you previously selected the installation option **Container (podman)** and placed the database on the same server with Device Monitor, then enter the address of the network interface of this server. Before this, configure the database (see Preparing the Environment).

    Important!

    If you selected the installation option **Container (podman)**, you cannot enter `localhost` or `127.0.0.1` as an IP address.
31. Specify the port for configuring interaction. If you do not specify it, the default `5432` port will be used.
32. Enter the name of the database. By default – `iwdm`.

33. Enter the name of the DBMS user. By default – `postgres`.
34. Enter the password.
35. Select **Yes** to install the distribution service. In this case, the distribution point will be able to spread the agent distribution kits to workstations. If you previously selected the **Container (podman)** server installation option, then the distribution service will also be installed with the containerisation support.
36. Specify the path to the PFX file of the key that encrypts the channel between the Device Monitor Server and the agents. If you do not specify the path, then the default `/opt/iw/dmserver/ssl.pfx` path will be used.
37. If you are installing the Server to the new database, then you need to create the encryption key. Select **Yes**.
38. Next, you can select the deployment type:
    a. **Interact with Traffic Monitor** – with the option to send events to Traffic Monitor;
    b. **Operate autonomously** – autonomous work without integration with Traffic Monitor.

    Important!

    When selecting the autonomous work mode, no predefined rules will be created in the policies by default.

    Note:

    After the installation, you can switch the autonomous mode in the section **Settings** → **Device Monitor servers**.
39. If you selected **Interact with Traffic Monitor** on the previous step, then enter the name of the server or its IP address.

    Important!

    The server name may contain Latin letters from "a" to "z" (case-insensitive), numbers from "0" to "9", and the hyphen "-". It cannot consist of numbers only. We recommend using the server name that starts with a letter.

    Note:

    If you need to change the InfoWatch Traffic Monitor address after the installation, you can do it in the Device Monitor server database:
    - the field `TRAFFIC_MONITOR_POLICY_SERVER_ADDRESS` of the table Settings contains the address of the Traffic Monitor server that is used by all servers of the Device Monitor pool (both primary and secondary) to obtain the Traffic Monitor policy and distribute it to the agents;
    - the `TmAddress` field in the ServerOption table contains the address of the Traffic Monitor server to which events from Device Monitor are sent. In this table, the `TmAddress` field may appear multiple times (depending on the number of servers in the pool).
40. If an access token to Traffic Monitor is requested, enter its value.
    To successfully connect the Device Monitor Server with the Traffic Monitor Server, you need to configure the remote server certificate validation (see Configuring Validation of the Remote Server Certificates).
41. If you selected **Update an existing database**, a check if there are rules that do not support configuration in the new version of Device Monitor is launched. If unsupported rules are detected, the migration will fail. In this case, we recommend contacting the InfoWatch technical support.
42. If you selected **Update an existing database** and plan to use the Device Control module, rules, and white lists, select **Using Device Control is required, migrate rules and white lists**. Wait until

the Device Control rules and white lists are migrated to the new version. If you do not plan to use Device Control, select **Using Device Control is not required, delete rules and white lists**.

43. Enter the IP address of the Device Monitor server.
44. During the initial installation of the Device Monitor Server and the database, you can load a custom configuration file with default policies and settings. To load the file, enter the path to it, such as `/root/configuration.zip`. In this case, all existing settings and configuration elements will be replaced with the imported ones.
    To skip this step, press **Enter**.

    > **Important!**
    >
    > The configuration file needs to be placed on a local disk or external storage device. Loading the file from a network folder is not supported.

45. Wait for the installation to complete.
    If you are installing in "All-in-one" mode to the office node of the Platform and have previously selected the **DM Server Service**, **Front End** option, the following actions will be performed automatically:
    - the public key of the **guard** service of the Platform will be obtained and recorded in Device Monitor. The key is required for the correct interaction between the web interface and the Server;
    - the **n.yaml** file will be corrected.

      > **Important!**
      >
      > Any product that will be installed in the Investigation Centre after Device Monitor will generate a new **n.yaml** file, and the section that is necessary for the correct interaction of the web interface with the Server will be deleted from it. To restore **n.yaml**, follow the steps 46a-46d.

46. If you install the web interface on the Platform basis and the Device Monitor Server in sequence, using the **Front End only** and **DM Server Service only** installation options, the actions involving the Platform's **guard** service key and the **n.yaml** file from the previous step will not be performed automatically. After installation, perform them using the installer. To do this:
    a. Run the installation script:

    ```
    ./setup.sh
    ```

    b. Select **Utilities** from the menu.
    c. Select **Fix n.yaml file**.
    d. Enter the IP address of the Device Monitor server and wait for the process to complete.
    e. Run the installation script:

    ```
    ./setup.sh
    ```

    f. Select **Utilities** from the menu and then **Save platform guard public key to IWDM Service**. Wait for the process to complete.
    g. Restart the **iwdms** service:

    ```
    systemctl restart iwdms
    ```

5.4.3 Installation of a secondary server

Regardless of the installation mode, you can install one or more secondary servers in addition to the primary one.

To install the Device Monitor secondary server:

1. Make sure the server meets the hardware and software requirements (see Hardware and Software Requirements).

2. Follow the steps to prepare the server for Device Monitor installation (see Preparing the Environment).
3. Copy the archive containing the Device Monitor Server distribution kit to the hard drive.
4. Create a directory and unpack the contents of the archive into it. In the example, the archive will be unpacked into the `/dmsl_distr` directory:

```
mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.0.310.tar.gz -C /dmsl_distr
```

5. Go to the created directory.
6. Run the **setup.sh** script, which is included in the distribution kit:

```
./setup.sh
```

> **Note:**
>
> If you encounter a permission error when running the script, make the file executable using the command:
>
> ```
> chmod +x ./setup.sh
> ```
>
> Then run the script.

7. Select **Install**.
8. Select **DM Server Service only**.
9. Select the Device Monitor server installation option:
   - **Host**, to install the server on a host; or
   - **Container (podman)**, to install the server with containerisation support.
10. Select the language of the server being installed and press **Enter**. This will determine the names of the preinstalled groups, policies, and rules.
11. Read the license agreement and select the required action. To continue the installation, you need to accept the license agreement. Select **Accept and continue** and press **Enter**.
12. Select the **Secondary** server type to install.
13. Specify the name or the IP address of the server where the PostgreSQL DBMS is located.
    Here and below, specify the same DBMS parameters that you specified when installing the primary server.
14. Specify the port for configuring interaction. If you do not specify it, the default `5432` port will be used.
15. Enter the name of the database. By default – `iwdm`.
16. Enter the name of the DBMS user. By default – `postgres`.
17. Enter the password.
18. Select **Yes** to install the distribution service. In this case, the distribution point will be able to spread the agent distribution kits to workstations. If you previously selected the **Container (podman)** server installation option, then the distribution service will also be installed with the containerisation support.
19. Wait for the installation to complete.

If the installation is successful, the Device Monitor Server service will be started. The service will be marked as automatically starting. To check whether the Device Monitor server service is running, run the command:

```
systemctl status iwdms
```

Next, go to the Investigation Centre. To connect to the web interface of the Investigation Centre, **always** use the address or name of the server where the **Platform is installed in** `central` **mode**. If the product in `central` mode is installed on the office node of the Platform, still use the `central` node of the Platform for work.

5.4.4 Preparing the Device Monitor Server for Migration from Windows to Linux-based Operating Systems

If you need to migrate data when switching from Windows to Device Monitor for Linux, follow these steps:

> **Important!**
>
> Do not delete the primary Device Monitor server until you have made sure that migration is supported.

1. Update Device Monitor installed in Windows to version 7.21 (see "Documentation for InfoWatch Device Monitor installed on MS Windows OS", article "Updating InfoWatch Device Monitor Server End").
2. Make sure that the Database is created and installed with the **support of the Russian locale**. This is required for the web interface to function correctly and for searching objects using Cyrillic characters within it. To check the locale, run the command:

   ```
   psql -l
   ```

   The locale is specified in the columns `LC_COLLATE` and `LC_CTYPE` of the row in the target database, for example:

   ```
                        List of databases
       Name    | Owner   | Coding    | LC_COLLATE    |  LC_CTYPE     |      Access
   rights
   ----------+-----------+-------------+--------------+--------------
   +------------------------
    iwdms     | postgres  | UTF8        | ru_RU.UTF-8  | ru_RU.UTF-8  |
   ```

3. Make sure that the Database supports data migration, meaning it does not contain the rules that are not supported in the new version. To do this:
   a. In the distribution kit along the path `7.21.x\DM for Windows\Utils`, copy the archive `CheckMigration.zip`.
   b. Unpack the archive.
   c. In the file run.bat, specify the parameters for accessing the Database. Add a line, if it is missing, and specify the current values for `IP`, `PORT`, `DB_NAME`, `USER_NAME`, `PASSWORD`:

      ```
      "CheckMigration.exe" --Server <IP>:<PORT> --DBName <DB_NAME> --User
      <USER_NAME> --Password "<PASSWORD>" --Culture "ru-RU"
      ```

      Example:

      ```
      "CheckMigration.exe" --Server 10.20.30.40:1234 --DBName iwdms --User
      postgres --Password "pass123" --Culture "ru-RU"
      ```

   d. Run the file `run.bat` from the computer where the Device Monitor primary server is installed.
   e. Wait for the message informing that you can start the migration: *The database is ready for migration*.
   f. If the utility outputs the list of rules that are not supported in the new version, delete these rules.
   g. If, after verification, you see an error telling that the Database is installed with the wrong locale, then follow the step 2 to verify it and make sure that Russian locale is installed. Otherwise, change it (see Checking and modifying the PostgreSQL database locale).
4. Delete all Device Monitor servers, leaving the Database intact and preserving the server's secret key. To do this, follow the instructions for your product version.

Rules that are not supported in the new version:

- control of messengers: MMP, Facebook, Skype;
- control of copying from/to CD/DVD;
- application control: launch prohibition, using the clipboard and printing.

Unsupported settings:

- parameters of AD and servers connection to which is permitted;
- automatic Agent updates;
- code generation key.

Migration of the connection setting for receiving the control commands from Activity Monitor is not supported.

5.5 Configuring Validation of the Remote Server Certificates

The ability to verify the certificates of remote servers is implemented on the Device Monitor server to enhance security. With this verification, you can ensure the authenticity of the remote server when connecting to it.
Traffic Monitor verifies the following certificates:

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

To successfully connect to a remote server to send events:

1. Configure certificate verification on the Traffic Monitor server.
2. On the Device Monitor server, install the root certificate of the remote server in the root certificate store at the "local computer" level.

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

1. Configure certificate verification on the
   This page has not yet been translated to English.
   server.
2. At your company's certification center, issue an X.509 certificate for the Traffic Monitor web server.
3. Configure the Traffic Monitor web server to work with the issued certificate.
4. Install the Traffic Monitor web server's root certificate at the "local computer" level root certificate store on the Device Monitor server.

Important!

If you do not perform steps 2–4, then you need to disable the verification of the Traffic Monitor web server certificate. Connection with the Traffic Monitor server will be protected with the TLS protocol, but the Device Monitor server will not be able to verify that it has connected to the right Traffic Monitor server.

5.5.1 Verifying the certificates of remote servers when establishing an SSL session

To configure the verification of remote server certificates when establishing an SSL session, set the value to `True` or `False` for the following fields in the Settings table in the Device Monitor server database:

- `IGNORE_SSLERR_TMXAPI_CONNECTION` – ignore the Traffic Monitor XAPI service certificate verification;
- `IGNORE_SSLERR_TMCONFIG_CONNECTION` – ignore the Traffic Monitor TMConfig certificate verification;
- `IGNORE_SSLERR_PLATFORM_CONNECTION` – ignore the certificate verification for the EPEVENTS Platform service.

If the value is `False`, the certificate will be verified.

The default value of the `IGNORE_SSLERR_TMXAPI_CONNECTION` field:

- during the initial Device Monitor server installation – `False`, meaning that the Traffic Monitor XAPI service certificate verification is enabled;

- when updating the Device Monitor server version 7.9 and below – `True`, meaning that the check is disabled;
- when updating the Device Monitor server version 7.10 or higher, the value remains the same as it was before the update.

The default value of the `IGNORE_SSLERR_TMCONFIG_CONNECTION` field:

- during the initial Device Monitor server installation – `False`, meaning that the Traffic Monitor web server certificate verification is enabled;
- when updating the Device Monitor server – `True`, meaning that the verification is disabled.

The default value of the `IGNORE_SSLERR_PLATFORM_CONNECTION` field:

- during the initial Device Monitor server installation – `True`, meaning that the certificate verification is disabled for the EPEVENTS Platform service;
- when updating the Device Monitor server versions 7.9 and below – `True`, meaning that the check is disabled;
- when updating the Device Monitor version 7.10 and above, the value remains the same as it was before the update.

If the values of the parameters `IGNORE_SSLERR_TMXAPI_CONNECTION`, `IGNORE_SSLERR_TMCONFIG_CONNECTION`, and `IGNORE_SSLERR_PLATFORM_CONNECTION` were changed, then to make the certificate verification rules for remote servers take effect, restart the Device Monitor server service.

5.5.2 Installing the Traffic Monitor XAPI service certificate

To install the

This page has not yet been translated to English.

1. On the Traffic Monitor server, open the file `/opt/iw/tm5/etc/**xapi.conf**`.
2. In the section `ThriftServers` -> `xapi`, find the parameter `TrustedCertificatesPath`. The value of this parameter specifies the path to the root certificate file and its name. If a relative path is specified, it needs to be interpreted relative to the `/opt/iw/**tm5**` folder.
   The default value of the parameter `TrustedCertificatesPath` is: `/opt/iw/tm5/etc/cert/**trusted_certificates**`.
3. Copy the root certificate to the computer where the Device Monitor server is installed or will be installed. If you will be using or have installed the Device Monitor server in a Docker environment, copy it to the `/opt/iw/dmserver/**cert**` directory. Do not move the certificate file to other directories during the entire operation and functioning of the Device Monitor server.
4. Go to the directory where the root certificate was copied. When using Docker – to the `/opt/iw/dmserver/**cert**` directory.
5. Rename the root certificate to `tmca.crt`.
6. Enter the commands depending on the operating system and the use of containerization in the environment where the root certificate is being installed:
   - For RED OS:

     ```
     sudo cp tmca.crt /etc/pki/ca-trust/source/anchors/
     sudo update-ca-trust
     sudo update-ca-trust extract
     ```

   - For RED OS using Docker:

```
sudo cp tmca.crt /opt/iw/dmserver/cert
```

- For ALT OS:

```
su -
cp tmca.crt /etc/pki/ca-trust/source/anchors/
update-ca-trust
```

- For ALT OS using Docker:

```
su -
cp tmca.crt /opt/iw/dmserver/cert
```

- For Astra Linux:

```
sudo cp tmca.crt /usr/local/share/ca-certificates/tmca.crt
sudo update-ca-certificates
```

- For Astra Linux using Docker:

```
sudo cp tmca.crt /opt/iw/dmserver/cert/tmca.crt
```

Running the commands may take some time.

7. Restart the server service `iwdms`:

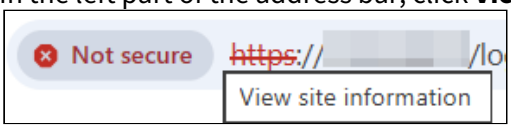
```
systemctl restart iwdms
```

XAPI service certificate:

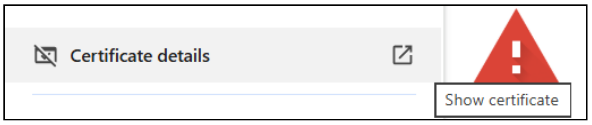
5.5.3 Installing the certificate of the Traffic Monitor web server

To install the certificate of the Traffic Monitor web server:

1. Open the Traffic Monitor Management Console in the browser.
2. Export the Traffic Monitor web server certificate from the browser. In our example, it is Google Chrome. To do this:
   a. In the left part of the address bar, click **View site Information**.



   b. Click **Show certificate**.



   c. In the Certificate Viewer, go to the *Details* tab.
   d. Click **Export**.
   e. Click **Save**.
3. Copy the root certificate to the computer where the Device Monitor server is installed or will be installed.
4. Go to the directory where the root certificate was copied.
5. Follow step 6 of the Traffic Monitor XAPI service certificate installation instructions described above, using the name of the previously copied root certificate of the Traffic Monitor web server instead of `tmca.crt`.

5.5.4 Installing the EPEVENTS Platform service certificate

To install the EPEVENTS Platform service certificate:

1. On the Platform server, get the root certificate `plca.crt` using the command:

   ```
   kubectl get secret -n infowatch epeventskeys-central -o 'go-
   template={{index .data "tls.crt"}}' | base64 -d > plca.crt
   ```

   If the Platform server is not the central server in the cluster, the command will look like this:

   ```
   kubectl get secret -n infowatch epeventskeys-<node label> -o 'go-
   template={{index .data "tls.crt"}}' | base64 -d > plca.crt
   ```

   where `<node label>` is the name of the server node.
2. Copy the root certificate to the computer where the Device Monitor server is installed or will be installed.
3. Go to the directory where the root certificate was copied.
4. Follow step 6 of the Traffic Monitor XAPI service certificate installation instructions described above, using the name of the previously copied root certificate of the Platform instead of `tmca.crt`.

Running the commands may take some time.

5.5.5 Viewing logs

If the Device Monitor server is unable to verify the certificate, an error will appear in the logs indicating 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 The certificate chain has been processed, but processing was
interrupted at the root certificate, which lacks a trust relationship with the trust
provider.

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

UntrustedRoot The certificate chain has been processed, but processing was
interrupted at the root certificate, which lacks a trust relationship with the trust
provider.
```

The interval between sending error messages to the log is determined by the values of the `WRITE_SSLVERIFY_TMXAPI_LOG_INTERVAL`, `WRITE_SSLVERIFY_TMCONFIG_LOG_INTERVAL`, and `WRITE_SSLVERIFY_PLATFORM_LOG_INTERVAL` fields in the Settings table of the Device Monitor server database. By default, these values are set to 3600 seconds. If the remote server certificate fails the verification again and less time has passed since the last error message was sent, a new error message will not be sent.

To view the logs:

1. Go to the folder `/opt/iw/dmserver/log`
2. Open the file `iwdms-<date>.txt`, where `<date>` is the date in the `YYYYMMDD` format.

5.6 Installing Device Monitor Agents

The Device Monitor Agent and the Device Monitor Server must be configured in the same time zone. This will ensure that the correct time of event interception is displayed.

Important!

Do not install the Device Monitor Agent and the Device Monitor Server on the same computer; this may cause the server to become inoperable.

5.6.1 Methods for installing the Device Monitor Agent

InfoWatch Device Monitor Agents can be installed on workstations in one of the following ways:

- Local installation. It is performed using a universal installer directly on each computer:
  - Local Installation of the Agent on a Workstation Running Windows
  - Local Installation of the Agent on a Workstation Running a Linux OS
  - Local Installation of the Agent on a Workstation Running Mac OS
- Installing Agents Using a Distribution Task. Performed in the InfoWatch Device Monitor web console.

Note:

Installing agents on workstations running MOS with a distribution task is not supported.

5.6.2 Preparing for installation

To install or update the InfoWatch Device Monitor Agent, follow these recommendations:

1. Exclude the parallel use of third-party DLP systems.
2. **To install on Windows, add the following files of the InfoWatch Device Monitor Agent to the antivirus exclusions:**
   - `%SystemRoot%\SysWOW64\iwprn_x86.dll`
   - `%SystemRoot%\System32\iwprn.dll`
   - `%SystemRoot%\System32\tm.dll`
   - `%SystemRoot%\System32\Drivers\IWDMDV.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMFS.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMH.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMSHC.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMWFP.SYS`
   - `%SystemRoot%\System32\Drivers\IwNNwF.SYS`
   - `%SystemRoot%\System32\IWDeployAgent.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\7z.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\rmtdiag.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwscrctl.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwshcs.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwdmc.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\IWProxy\IWProxy.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\IWProxy\SystemCertificate\updroots.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\DM.Client.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\Client.RebootReminder.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwmediarec.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwdmifilter.exe`

   where `%ProgramFiles%\Infowatch\DeviceMonitor\Client\` **is the default**

installation path for the Agent. If you use different paths when installing different groups of workstations, take all of them into account.

We also **recommend** to add the following exclusions:

- **Agent installation folder**. By default: `C:\Program Files\Infowatch\DeviceMonitor\Client\`
- **Folder for storing shadow copies**: `_IWEVT_{3FF1ABF9-77EE-411c-A698-ECA23E44A3BF}_`. This will help reduce the load. The folder can be located on any volume that has sufficient free space.

3. **To install on Linux-family OS, add the following InfoWatch Device Monitor Agent files to the antivirus exclusions:**

   All files in folders and subfolders:

   - `/sys/module/iwdmfsshc/`
   - `/sys/module/iwdmnfredir/`
   - `/opt/iw/dmagent/`
   - `/opt/iw/deployagent/`
   - `/opt/iw/share/config`

   We also **recommend** to configure process exclusions. Exclude processes with the following paths (including child processes):

   - **`/sys/module/iwdmfsshc/*`**
   - **`/sys/module/iwdmnfredir/*`**
   - **`/opt/iw/dmagent/*`**
   - **`/opt/iw/deployagent/*`**
   - **`/opt/iw/share/config/*`**

4. Disable the antivirus's self-protection.
5. If possible, disable or uninstall the antivirus during the installation, update, and deletion of the InfoWatch Device Monitor Agent.
6. If VMware Horizon VDI 8.0.0-16530 is used on workstations, the ftapihook654.dll component version 3.2.4.1 must be disabled (see VMware Horizon VDI compatibility issues).
7. **On workstations running Astra Linux, disable some OS settings during the remote installation of Agents**

   To do this:

   a. Disable the blocking of interpreters other than bash using the command:

   ```
   sudo astra-interpreters-lock disable
   ```

   b. Disable the blocking of the bash interpreter using the command:

   ```
   sudo astra-bash-lock disable
   ```

   c. Disable the prohibition on setting the execute bit with the command:

   ```
   sudo astra-nochmodx-lock disable
   ```

   Note:

   After installing the Device Monitor Agents, you can revert the modified settings to their original values. To do this, run the same commands, replacing `disable` with `enable`. For more information about the Astra Linux security settings, see the documentation on the official website.

8. Ensure access to the ports required for the InfoWatch Device Monitor Agent to work (see the list of ports in *InfoWatch Traffic Monitor*. *Administration Guide*, section *Configuring InfoWatch Device Monitor Server*).
9. **To quickly obtain the FQDN of a workstation running a Linux OS, make sure the following parameters are configured before installing the Agent:**
    a. The file `/etc/hostname` contains:
        - the name of the host, such as `computer-20`
          or
        - FQDN name, such as `computer-20.corp.ad`
    b. The file `/etc/hosts` defines the correspondence between the host name, FQDN, and IP address:
        - if the host name is defined on the workstation and the workstation has a FQDN name, then the file must contain the following line:

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

          where `<FQDN name>` is the FQDN name;
          `<hostname>` is the host name.
          For example, for the host name `computer-20` and the FQDN name `computer-20.corp.ad`, the line would look like this:

          ```
          127.0.1.1 computer-20.corp.ad computer-20
          ```
        - if the workstation does not have a FQDN name, the file must contain the following line:

          ```
          127.0.1.1 <hostname>
          ```
        - if the file `/etc/hostname` contains a FQDN name, then the file must include the following line:

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

          Note:
          The IP address value in the line can be 127.0.1.1 or 127.0.0.1.

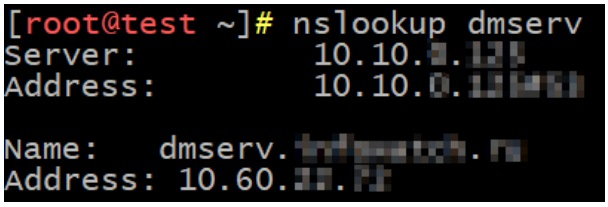
          Note:
          The listed parameters can also be configured using third-party software, such as the *Domain Join* program.

          To avoid errors when adding a host to Active Directory, the following requirements apply to the host name:
            - the following characters are allowed: Latin alphabet symbols (`A` - `Z` , `a` - `z`), digits (`0` - `9`), and a hyphen;
            - the name length must be no more than 15 characters.
10. To establish a connection between the InfoWatch Device Monitor server and the workstation on which the InfoWatch Device Monitor Agent is installed, their domain names need to be correctly resolved by the DNS server into IP addresses. Verify this using the command:

    ```
    nslookup <host_name>
    ```

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

```
nslookup dmserv
```



If the execution of this command results in the error **`server can't find dmserv: SERVFAIL`** for the InfoWatch Device Monitor server, the connection will not be established.

> **Note:**
>
> Additionally, to establish a connection between the InfoWatch Device Monitor Agent and the InfoWatch Device Monitor server, you can add the following line to the `/etc/hosts` file on the workstation where the Agent is being installed:
>
> ```
> <IP_address_of_the_Device_Monitor_server> <Device_Monitor_server_name>
> ```

If you encounter any difficulties with configuring network settings, contact your system administrator.

11. If you do not need to use the network connection control component, disable it when creating the InfoWatch Device Monitor Agent distribution.
12. First, install the InfoWatch Device Monitor Agents on test machines or a small group of workstations.
    If no errors, performance degradation, or application freezes occurred on the test group within 2–3 days, continue the installation on the workstations.

Important!

Note that during the Agent installation process:

- Turning off the computer's power supply may lead to errors that cause unstable operation of the operating system. This also applies to the processes of deleting the Agent.
- A short-term disruption of all network connections is performed. This is due to the installation of network traffic control components used in Device Monitor (IWPROXY and IWNBG). In addition, the disruption is related both to the technological features of the OS when installing modules and to the forced restart of network cards when installing the "transparent proxy" module. This also applies to the processes of deleting and updating the Agent.
- The Mozilla Firefox and Mozilla Thunderbird programs will be closed (if they were running).

If the workstation is configured to connect to the corporate network remotely (via a VPN agent), add the VPN agent to the interception exceptions (including network interception).
The InfoWatch Device Monitor Agent is launched automatically immediately after installation. Until the computer is restarted, the Agent's functionality is limited to:

- intercepting traffic passing through a proxy server;
- network interception (when the Agent is installed on Windows 8 and later);
- interception of copying to external storage devices.

When the Secure Boot protocol is enabled, loading the kernel-mode module is not guaranteed.

Important!

If you are installing the Agent on a workstation running Windows 7 Service Pack 1 or Windows 2008 R2 Server:

- install the Windows update packages for the specified OS. See Hardware and Software Requirements.
- note that if the Agent is installed for the first time, the *Corporate Network Control* component will not be installed. If necessary, you can do it manually using the command line.

Important!

On **Linux** operating systems, you cannot independently delete or modify the accounts listed below, as this will cause the InfoWatch Device Monitor Agent to become non-functional:

- `iwdm` – used by the main Device Monitor service;
- `iwdeployagent` – used by the Device Monitor agent distribution service;
- `iwregistry` – currently not in use.

  Accounts are created in the operating system when the Agent is installed to restrict access to Device Monitor data. When the Agent is uninstalled, the specified accounts will be automatically deleted.

5.6.3 Local Installation of the Agent on a Workstation Running Windows

Important!

We strongly recommend not to install InfoWatch Device Monitor Agents on computers with the same names. Such computers will be registered as a single computer, and accordingly, they will be subject to the same policy, shared event registration, and so on.

Obtain and write the current package for installing the Agent to an external storage device. A user who has local administrator rights on that computer can perform the installation.

Installing the Device Monitor Agent on a computer running Microsoft Windows using an MSI package, followed by manual input of parameters

1. **Launching the installation wizard**

   Insert the external media with the Agent distribution kit into the computer. Then open the `Client` folder. In this directory, find and launch the installation package for the required platform for deployment in accordance with the parameters specified when generating the packages, such as `InfoWatch.DeviceMonitor.Client.7.21.0.x64.msi`

   Note:

   Starting from **Device Monitor version 7.18.5, during the initial installation of the Agent**, the installer checks whether the list of applications that should be excluded from interception was received. If the list of exclusions was not received, the installation of this Agent will be stopped. In this case, the log will contain the entry `CustomAction GetExclusionsFromServerWithCheck returned actual error`.

   Disabling this check is only available when installing via the command line.

   As a result, the InfoWatch Device Monitor Client installation wizard's welcome window will be displayed on the screen. Click "Next" to proceed to the next window.

2. **Selecting the installation directory**

   Specify the path to the folder where the **Agent** will be installed.

   Important!

   The folder path may contain the following characters:

   `0-9` , `a-z` , `A-Z` , `:` , `.` , `_` , `-` , `\` , ` `

   If there are other characters in the path, the Agent installation will be incorrect.

Click **Next**.

3. **Configuring the parameters**
   Specify the parameters for connecting with the InfoWatch Device Monitor Server:
   - **Server.** Name of the InfoWatch Device Monitor Server.
   - **Port**. The port number used for the connection between the InfoWatch Device Monitor Agent and the Server (the default port is 15101).

   Click **Next**.
4. **Completing the installation**
   After going to the **installation confirmation** window, click **Next** to start the Agent installation. Follow the wizard's instructions to complete the installation. After the installation is complete, reboot the computer.

Installing the Device Monitor Agent on a computer running Microsoft Windows using an MSI package in silent mode

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

Before running the installer:

1. Insert the external media with the Agent distribution kit into the computer.
2. Launch the command line (`cmd.exe`) as an Administrator.
3. Navigate to the directory where the Agent distribution kit is located by running the command:

```
cd <path_to_the_distribution_kit>
```

Review the list of keys in the table below. You can use them to specify the product installation parameters for the installer.

Key	Description
`/quiet`	Running the installation without displaying the user interface.
`/i <installation_package_name>`	Running the product installation using the specified file.

`PREDEFINED_CLIENTDIR`	Directory for product installation.
	Default value:
	`"%ProgramFiles%\Infowatch\DeviceMonitor\Client"`
	Important!
	The path to the folder may contain the following characters:
	`0-9` , `a-z` , `A-Z` , `"` `:` `"` , `"` `.` `"` , `"` `_` `"` , `"` `-` `"` , `"` `\` `"` , `"` `"`
	If there are other characters in the path, the Agent installation will be incorrect.

Key	Description
`UNINSTALL_PASSWORD_SHA1_HASH`	The hash value of the uninstallation password in hexadecimal format, calculated using the SHA-1 algorithm. If this parameter is set, the Device Monitor Agent can only be deleted by entering the correct password. **Important!** The password hash value must be calculated for the UTF-16LE Unicode encoding. Specify the hash value using only uppercase letters and numbers.
`IWPROXYDN`	A string containing the domain name of the root certificate of the proxy server on the workstation, which is used to issue certificates when intercepting secure traffic. The name must comply with the X.509 standard and contain the CN (Common Name) field. Fields within the name must be comma-separated. Default value: `"CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow"`
`SHOW_USER_NOTIFICATION`	Show the user a notification about the need to reboot the computer. Possible values: • `"#x01000000"` (by default) – show; • `"#x00000000"` – do not show.
`WAITING_REBOOT_PERIOD`	The waiting time for the workstation to reboot until the Agent starts showing the notification about the need to reboot. Specified in hours. Default value: `"0"`
`REBOOT_NOTIFICATION_PERIOD`	The time until a forced reboot, during which the Agent displays a notification about the need to reboot. Specified in hours. Possible values: • integers from 0 to 1000; • `"-1"` (default) to display the notification indefinitely and not force a reboot of the computer.

Key	Description
`REBOOT_NOTIFICATION_RATE`	The frequency at which the Agent displays a notification about the need to reboot. Specified in minutes. **Note:** If the parameter is not set, the notification is displayed every 10 minutes.
`REBOOT_NOTIFY_MESSAGE`	Text of the notification about the need to reboot the computer. The message can contain no more than 255 characters. Default text: "`Reboot the computer as soon as possible`"
`FORCE_REBOOT`	Sending a final notification before a forced reboot. Possible values: `"0"` (default) – show the final notification; `"1"` – do not show the final notification. **Important!** After the final notification, the employee will have 5 minutes to finish their operations. If the parameter is set to `"1"`, then a forced reboot (if it is set by the `REBOOT_NOTIFICATION_PERIOD` parameter) will be performed unexpectedly for the employee.
`HIDE_CLIENT`	Hide the Device Monitor Agent's presence from the workstation user. Possible values: • `"#x01000000"` – hide the Agent; • `"#x00000000"` (default) – do not hide the Agent. **Important!** Failure to notify about the use of interceptors may conflict with the current legislation of your country. **Important!** The notification about the need to restart the computer will not be displayed if the value of this parameter is set to `"#x01000000"` – hide the Agent.
`NOIWPROXY`	Do not install the network traffic interception component. Possible values: • `"0"` (default) – install the component; `"1"` – do not install the component.

Key	Description
`NOIWNBG`	Do not install the network connection monitoring component. Possible values: • `"0"` (default) – install the component; • `"1"` – do not install the component.
`SRVPOOL`	List of the Device Monitor servers that the Agent can connect to. Specified in the following format: `<Server>[;<Server>[;<Server>[{*};{*}...]]]` where `<Server> = <DNS server name>:<port number>` Example parameter value: `"dmserver:15101;"` If the Agent cannot connect to the first server in the list, it will attempt to connect to the next one in the list, and so on. After connecting to the server, the Agent will be linked to it.
`EXCL_REQUIRED`	Starting from **Device Monitor version 7.18.5, during the initial installation of the Agent**, the installer checks whether the list of applications that should be excluded from interception was received. If the list of exclusions was not received, the installation of this Agent will be stopped. In this case, the log will contain the entry `CustomAction GetExclusionsFromServerWithCheck returned actual error`. If you want to disable the check, add the `EXCL_REQUIRED = 0` option to the launch command.
`/lvp <log_file_name>`	Write data to the specified log file.

To install the InfoWatch Device Monitor Agent:

1. In the command line, run the Agent installation program with the specified parameters.
   Example of the installation command:

```
%windir%\system32\msiexec.exe /quiet /i
InfoWatch.DeviceMonitor.Client.x64.ru.7.21.0.192.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.7.21.0.192.log
```

2. Wait for the installation to complete.
3. Reboot the computer.

5.6.4 Local Installation of the Agent on a Workstation Running a Linux OS

Important!

We strongly recommend not to install InfoWatch Device Monitor Agents on computers with the same names. Such computers will be registered as a single computer, and accordingly, they will be subject to the same policy, shared event registration, and so on.

Note:

We do not guarantee the correct installation of the Agent if there is a customized version of the SELinux system installed on the computer.

1. **Preparing for the installation:**
   a. Make sure that the user who will install the system has the required permissions:
      - on a computer running OS ALT Workstation – the permissions to execute `su`;
      - on a computer running other Linux family operating systems – the `sudoers` privileges.
   b. Copy the archive that contains the package and scripts for installing and uninstalling the Device Monitor Agent to your computer. The archive is included in the distribution kit. The name of the archive may vary depending on the OS being used:
      - `Setup.AstraLinux-1.7-iwdm.x86_64.x.x.x.xx.tar.gz` – for Astra Linux Special Edition 1.7;
      - `Setup.AstraLinux-1.8-iwdm.x86_64.x.x.x.xx.tar.gz` – for Astra Linux Special Edition 1.8;
      - `Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.tar.gz` – for RED OS 7.3.1;
      - `Setup.RedOS-8.0-iwdm.x86_64.x.x.x.xx.tar.gz` – for RED OS 8.0;
      - `Setup.AltLinux-10.0-iwdm.x86_64.x.x.x.xx.tar.gz` – for ALT Workstation 10;
      - `Setup.AltLinux-11.0-iwdm.x86_64.x.x.x.xx.tar.gz` – for ALT Workstation 11;
      - `Setup.Rosa-12.5.1-iwdm.x86_64.x.x.x.xx.tar.gz` – for MOS.

      where `x.x.x.xx` is the build number.
      Next, we will look at an example of installing the Agent on RED OS 7.3. Installation on ALT, Astra Linux, and RED OS 8.0 is similar. Examples of commands for ALT and Astra Linux are provided below.
      To install the Agent on a workstation running MOS, see a separate instruction.
   c. Go to the directory where the archive was copied and enter the command to unpack it:

```
sudo tar -xvzf Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.tar.gz
```

   As a result, files `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<agent_version>.deb` will be created.
2. **Installing the InfoWatch Device Monitor Agent:**
   a. Go to the directory where the contents of the `Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.tar.gz` archive were unpacked.
   b. To install the Agent, run the script by executing the command:
      - For a standard installation (this will install the network traffic interception component):

```
sudo ./install.sh <server>:<port> [-g '<Proxy_DN>']
```

where `<server>` is the IP address or the domain name of the InfoWatch Device Monitor Server, `<port>` is the port for connecting to the InfoWatch Device Monitor Server,
`[-g '<Proxy_DN>']` is the optional parameter for explicitly specifying the DN (Issuer Distinguished Name). Use it if you want to set the DN for the proxy certificate. Name `<Proxy_DN>` should contain the field CN (Common Name). The fields within the name should be coma-separated.

> **Note:**
>
> The BT name by default: `' CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow'`
>
> If you do not use the `-g` parameter or specify the default value, the DN in the generated connection certificate will be as follows:
> `CN = IWDMProxy(<machine_uuid>)`
> `OU = Infowatch TechDep`
> `O = Infowatch`
> `L = Moscow`
> `ST = RU`
> `C = RU`
>
> where `<machine_uuid>` is the identifier of the workstation created by the Agent.

In our example, the command will be as follows

```
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, during the initial installation of the Agent**, the installer checks whether the list of applications that should be excluded from interception was received. If the list of exclusions was not received, the installation of this Agent will be stopped. In this case, the log will contain the entry:
>
> ```
> D: Exit status: 0
> [infowatch-agent-install] postinst: ERROR: exclusions not received (rc=255); abort install (exit 2)
> ```
>
> If you want to disable the check, add the `IW_EXCL_REQUIRED=0` option to the launch command.
>
> **Example of an Agent installation command without checking the exception list:**
>
> ```
> sudo IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101
> ```

> **Note:**
>
> To display the help section, run the command:
>
> ```
> sudo ./install.sh -h
> ```

- To install without the network traffic interception component:

```
sudo IWDM_NO_PROXY=1 ./install.sh <server>:<port>
```

c. You can check the status of the services with the command:

```
sudo systemctl status "iwdm*"
```

> **Note:**
>
> If you choose not to install the network traffic interception component, then:
> - `iwdmproxy` service will not be started;
> - `no_proxy` file will be created in the `/opt/iw/dmagent/etc/iwdmproxy` directory;
> - when updating the Agent, the network traffic interception component will also not be installed.

d. Restart the workstation with the command:

```
reboot
```

Examples of commands for other operating systems

Astra Linux:

1. Unpacking the archive:

```
sudo tar -xvzf Setup.AstraLinux-1.7-iwdm.x86_64.x.x.x.xx.tar.gz
```

2. Launching the installation:

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

Example of the Agent installation command without checking the exception list:

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

In the case of installation without the network traffic interception component:

```
sudo IWDM_NO_PROXY=1 ./install.sh dm-server:15101
```

3. Checking the status of services:

```
sudo systemctl status "iwdm*"
```

OS ALT:

1. Unpacking the archive:

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

2. Launching the installation:

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

Example of the Agent installation command without checking the exception list:

```
su -c "IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101"
```

In case of installation without the network traffic interception component:

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

3. Checking the status of services:

```
su - -c 'systemctl status "iwdm*"'
```

Installing the Agent on a workstation running MOS

1. Go to the directory where the archive was copied and enter the command to unpack it:

```
sudo tar -xvzf Setup.Rosa-12.5.1-iwdm.x86_64.x.x.x.xx.tar.gz
```

As a result, the `/depends` directory and the files `iwdm-<agent_version>.rpm`, `iwfiles.sign`, and `iwfiles.digests` will be created.

2. To install the Agent, install the RPM package by running the command:

```
rpm -i iwdm-<agent_version>.rpm
```

The product will be installed in the directory `/opt/iw/dmagent`

3. Run the script `/opt/iw/dmagent/bin/first_run.sh`:

```
/opt/iw/dmagent/bin/first_run.sh <server>:<port>
```

where `<server>` is the IP address of the InfoWatch Device Monitor Server, `<port>` is the port for connecting to the InfoWatch Device Monitor Server.
In our example, the command will be as follows:

```
/opt/iw/dmagent/bin/first_run.sh dm-server:15101
```

4. You can check the status of the services with the command:

```
sudo systemctl status "iwdm*"
```

5. Restart the workstation with the command:

```
reboot
```

5.6.5 Local Installation of the Agent on a Workstation Running Mac OS

Important!

We strongly recommend not to install

This page has not yet been translated to English.
Agents on computers with the same names. Such computers will be registered as a single computer, and accordingly, they will be subject to the same policy, shared event registration, and so on.

Important!

Installation via SSH is not allowed.

1. **Preparing for installation:**
   a. Make sure that the user on whose behalf the installation will be performed has the `sudoers` privileges.
   b. Copy the archive containing the package and scripts for installing and uninstalling the Device Monitor Agent to your computer.
   In our example, it is `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 where the archive was copied and enter the command to unpack it:

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

   As a result, the files `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<agent_version>.pkg` will be created.
2. **Installing the InfoWatch Device Monitor Agent:**
   a. Go to the directory where the contents of the archive `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz` were unpacked.
   b. To install the Agent, run the script by executing the command:

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

   In the command above:
   `<server>` is the IP address or the domain name of the InfoWatch Device Monitor Server,
   `<port>` is the port for connecting to the InfoWatch Device Monitor Server.
   In our example, the command will be as follows:

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

   c. During the installation, the script makes changes to the system's trusted certificate settings. After running the script, the operating system will request permission for this action in a separate window. To confirm, enter your account password.
   Wait for the installation to complete. The product will be installed in the `/opt/iw/dmagent` directory.
   d. Check the service statuses using the following commands:

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

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

   e. Restart the workstation with the command:

```
reboot
```

5.6.6 Installing Agents Using a Distribution Task

Note:

Installing the Agent with a distribution task is possible only on workstations running Windows, Astra Linux, ALT, or RED OS.

To install Device Monitor Agents on workstations with the distribution task in the Device Monitor web console, you need to have a distribution service installed (see New Installation, step 34).

Before installing the Agents:

- We recommend adding the Agent files to antivirus exclusions. For the list of files, see List of InfoWatch Agent's files to be added to antivirus exclusions group.
- To distribute Agents to workstations running:
  - **Astra Linux Special Edition** versions **1.7** and **1.8:**
    For the user on whose behalf the Agent will be installed, configure the maximum level of mandatory access. For example, you can increase the access level for the `root` user with the command:

    ```
    sudo pdpl-user -i 63 root
    ```

  - **ALT Workstation 10**:
    For the user on whose behalf the task will be launched:
    i. Manually enable SSH access to the workstation with the command:

    ```
    service sshd start
    ```

    ii. In the file `/etc/openssh/sshd_config`, uncomment the line `PermitRootLogin`.
    iii. Add the user to the group `/etc/sudoers`.

To install the Agents:

1. In the section **Tasks** of the web console, create a primary distribution task. See *InfoWatch Device Monitor for Linux. User Guide*, article Primary Distribution and Updating Task.
2. Create a list of workstations for installing the Agents.
3. Run the task by clicking .
4. Enter the credentials of the user on whose behalf the task is being run and click **Run**.
5. Wait for the task to complete. The task status area will display a list of workstations with information about the Agents.
6. For the proper operation of the feature on a workstation running a Linux-based OS, restart the computer after installing the Agent.

Important!

The **Tasks** section will be disabled in subsequent versions. Installation, update, and deletion management is available in a new section with enhanced control and prioritization capabilities. See *InfoWatch Device Monitor for Linux. User Guide.* Distribution Policies.

Important!

Take the following into account:

- You cannot install the InfoWatch Device Monitor Agent and the Device Monitor server on the same computer, as this may lead to the server becoming inoperable.
- When installing, updating, or deleting the Agent, a short-term disruption of all network connections occurs. This happens because of the installation of network traffic control components used in Device Monitor (`IWPROXY` and `IWNBG`). In addition, the disruption is related both to the technological features of the OS when installing modules and to the forced restart of network cards when installing the *transparent proxy* module.

- If a customized version of the SELinux system is installed on the computer, the correct installation of the Agent is not guaranteed.

6 Configuring Network Access Rules

For the system to function properly, the following connections should be allowed:

Direction of the connection	Port	Purpose of the port
Ports required for the installation of the Device Monitor server and agents:		
Device Monitor server → DBMS server	PostgresSQL DBMS port	Interaction of the Device Monitor Server with the PostgresSQL DBMS (TCP 5432 by default).
Device Monitor server → Device Monitor Agent (Linux)	TCP 22	Installing the Device Monitor Agent on a workstation running a Linux-based OS.

Direction of the connection	Port	Purpose of the port
Device Monitor server → Device Monitor agent (Windows)	TCP 135	Installing the Device Monitor Agent on a workstation running a Windows-based OS. **Note:** * TCP port 593 may be used implicitly, in accordance with the OS settings of the Device Monitor server from which the distribution agent is deployed during the initial installation.
	UDP 137	
	UDP 138	
	TCP 139	
	TCP 593 *	
	TCP 445	
Device Monitor agent (Windows) → Device Monitor server	TCP 445	
Device Monitor server → Device Monitor agent (Linux\Windows)	TCP 15505	Communication with the Deploy Agent service (installation, updating, and deletion of the agent).
Device Monitor agent → Device Monitor server (distribution service)	TCP 15200	Initiating the loading of the Agent distribution kit from the Device Monitor Server to the workstation.

Direction of the connection	Port	Purpose of the port
Ports required for the operation of the Device Monitor server and agents:		
Administrator's workstation → Device Monitor server	TCP 22	Connection to the Device Monitor server via SSH.
Security officer's workstation → Central node of the Platform	TCP 443	Investigation Centre web console for managing Device Monitor.
Device Monitor server → Traffic Monitor server	TCP 443	Retrieving data protection policies on agents from Traffic Monitor.
Device Monitor server → Active Directory server	TCP 389 TCP 636 TCP 3268	Synchronization with Active Directory.
Device Monitor server → Traffic Monitor server	TCP 9100	Passing shadow copies to Traffic Monitor.
Device Monitor agent → Activity Monitor server	TCP 11008	Passing activity statistics events from the Device Monitor agent directly to Activity Monitor. You need to configure direct event sending to Activity Monitor.

Direction of the connection	Port	Purpose of the port
Device Monitor agent → Device Monitor server	TCP 15101	Initialization of a secure connection.
	TCP 15004	Passing shadow copies via an encrypted connection.
Device Monitor agent → Device Monitor server Device Monitor server → Device Monitor agent	UDP 15100	Internal Device Monitor protocol (passing statuses, notifications about settings changes, and so on).
Device Monitor server → Device Monitor agent	TCP 15506	Managing the Device Monitor agent (turning on and off, collection of diagnostic information).
Platform → Device Monitor primary server	TCP 15507	Interaction of the Platform with the primary Device Monitor server (with the WebAPI service installed).

Direction of the connection	Port	Purpose of the port
Device Monitor server → Activity Monitor server	TCP 17104	Passing shadow copies to Activity Monitor (screenshots, keylogger, device connection events). Also, activity statistics are passed via this port for agents version 7.15 and below, or if direct event sending to Activity Monitor is not configured.

Note:

If ports other than those specified in the table were assigned during the installation, they should be used. If you want to use the standard ports from the table afterwards:

a. Stop the Device Monitor server service with the command:

```
systemctl stop iwdms
```

b. To change the Device Monitor Server's ports for connection to the Agents, edit the parameters in the `ServerOption` table in the Device Monitor Server's database:

- `NotificationPort` (UDP 15100)
- `ClientFacadePort` (TCP 15101)
- `SSLPort` (TCP 15004)

c. Turn on the Device Monitor server service with the command:

```
systemctl start iwdms
```

7 Updating Device Monitor

Updating Device Monitor is performed in the same order as its installation:

1. Updating Device Monitor Server
2. Updating Device Monitor Agents

Note:

Starting from version 7.19, you can update the configurations of certain technologies without updating the Agents (see Updating Configuration on Device Monitor Agents).

7.1 Updating Device Monitor Server

Important!

Updating to version **7.21** is supported only by resetting the **Front End** component installation.
When updating from version **7.21.X** to version **7.21.5 or later**, the **direct** update is supported.
To update a cluster consisting of several servers, first update the **primary** Device Monitor server according to the instructions, and then the **secondary** servers.
Make sure that the database with which the Device Monitor server interacts has the Russian locale (`ru_RU.utf8`) installed. For details, see Checking and changing the PostgreSQL database locale.

Important!

When updating by resetting the installation, large amounts of data are reloaded into the ClickHouse OLAP DBMS, which is part of the Platform. This process may take a long time. In the Investigation Centre, events may temporarily not be displayed.

Sections of the article:

- Updating by resetting the installation
- Updating with a reset during a distributed installation
- Switching to a Server version with containerization support
- Direct updating the Device Monitor Server (when updating to version 7.21.5 or later)
- Updating Device Monitor Server running the Astra Linux OS (when updating to version 7.21.5 or later)

Updating the Device Monitor Server by resetting the installation
To update the Device Monitor Server:

1. Follow the steps to prepare the server for updating Device Monitor.

   Important!

   Make sure to install the Python version 3 interpreter and the additional packages for it, including `importlib-metadata` and `pyyaml` .
   Also make sure that the dotnet version is up to date.
   For details, see Preparing the Environment.

2. Copy the archive with the Device Monitor Server distribution kit to your hard drive.
3. Create a folder and unpack the contents of the archive into it. In our example, the archive will be unpacked into the `/tmp/dmsl_distr` folder:

   ```
   mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.21.0.402.tar.gz -C /tmp/
   dmsl_distr
   ```

4. Unpack the archive containing the Device Monitor Frontend version 7.21 distribution kit. In our example, the file will be extracted to the `/tmp/iwdm` folder:

   ```
   mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.21.0.402.tar.xz
   -C /tmp/iwdm
   ```

5. Go to the folder `/tmp/iwdm` and reset the Platform installation. If you have several InfoWatch products installed on different servers, run the command first on the **office** node of the Platform, then on the **central** node:

   ```
   ./setup.py reset
   ```

   Wait for the process to complete.
6. Restart the server with the command:

   ```
   reboot
   ```

   If you have multiple InfoWatch products installed, restart all servers.
7. To free up disk space, you can delete the `/tmp/iwdm` folder.
8. If you are updating by moving to another server or to a new OS, copy the folders containing the data specified during installation to another partition or to the new server.

   > **Note:**
   >
   > By default, folders are located along the **`/opt`** path.
   >
   > In **Device Monitor versions below 7.16**, folders were located along the **`/mnt`** path by default. Make sure to copy the folders while preserving permissions and owners. Use standard tools for copying, such as the `rsync` utility.
9. Make sure that at least 30 GB of disk space is available in the partition with the `/var/lib/containerd` folder.
   To check the available disk space, use the command:

   ```
   df -h /var/lib/containerd
   ```

   > **Note:**
   >
   > To free up disk space, you can delete the directory with container images from previous versions `/var/lib/containerd`. To do this, run the command:
   >
   > ```
   > rm -rf /var/lib/containerd
   > ```
   >
   > **This command deletes all container images. Do not use it if new versions of Device Monitor or other InfoWatch products are already installed on the server.**
10. Go to the folder `/tmp/dmsl_distr`
11. Make sure the server meets the hardware and software requirements (see Hardware and Software Requirements).
12. Run the script **setup.sh**:

    ```
    ./setup.sh
    ```

    > **Note:**
    >
    > If you encounter a permission error when running the script, make the file executable with the command:
    >
    > ```
    > chmod +x ./setup.sh
    > ```
    >
    > Then run the script
13. Select **Update**.

14. Select the option to update with reset – **Update all after you reset DM Front End: install DM Front End and update DM Server Service**.
    The DM Front End component will be installed on the Platform and the Device Monitor Server will be updated.
15. Select the Platform installation mode – **Central** (or **Office** in case of a distributed installation).
16. Next, follow the steps for installing the Platform from New Installation.
    When the installer asks you to specify the folders for storing data, specify the folders containing data of the previous version and select **n** when asked whether the folders should be cleared before installation.
17. Wait for the DM Front End installation and Device Monitor Server update to complete.
    The following actions will be performed automatically:
    - the public key of the Platform's **guard** service is retrieved and recorded in Device Monitor. It is required for the correct interaction between the web interface and the Server
    - the **n.yaml** file is fixed.

    > **Important!**
    >
    > Any product that will be installed in the Investigation Centre after Device Monitor will generate a new **n.yaml** file, and a section that is necessary for the correct interaction of the web interface with the Server will be deleted from it. To restore **n.yaml**, follow steps 18a–18c.
18. If you install the Platform-based web interface and update the Device Monitor Server separately, using the **DM Front End only** installation and the **DM Server Service only** update option, the actions involving the Platform **guard** service key and the **n.yaml** file from the previous step will not be performed automatically. After installing the Platform and updating the Server, perform them using the installer. To do this:
    a. Run the installation script:
    ```
    ./setup.sh
    ```
    b. Select **Utilities** and run the **Fix n.yaml file** item.
    c. Specify the IP address of the computer on which the Device Monitor Server was installed. If it was installed on the current computer, press **Enter**. Wait for the process to complete.
    d. Run the installation script:
    ```
    ./setup.sh
    ```
    e. Select **Utilities** from the menu and then **Save platform guard public key to IWDM Service**. Wait for the process to complete.
    f. Restart the **iwdms** service:
    ```
    systemctl restart iwdms
    ```
19. Update all installed **Secondary** Device Monitor Servers by performing the following steps on each of them:
    a. Run the script **setup.sh**:
    ```
    ./setup.sh
    ```
    b. Select **Update**.
    c. Select **DM Server Service only**.
    d. Wait for the update process to complete.

To make sure that the update is correct, go to the Investigation Centre web interface and check the availability of the section **Settings → Device Monitor → Servers**.
If you disabled sending notifications in Telegram before the update, enable it again.

Updating with reset during distributed installation

Initial conditions:

- Device Control version 1.4 and Activity Monitor version 3.5 are installed on the central node of the Platform;
- Device Monitor Server version 7.20 is installed on the office node of the Platform (in `central` mode).

To update the Device Monitor Server:

1. On the office node of the Platform, complete the steps to prepare the server for updating Device Monitor (see Preparing the Environment; make sure the dotnet version is up to date).
2. Copy the archive with the Device Monitor Server distribution kit to the office node.
3. Create a folder and unpack the contents of the archive into it. In our example, the archive will be unpacked into the `/tmp/dmsl_distr` directory:

```
mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.21.0.402.tar.gz -C /tmp/
dmsl_distr
```

4. Unpack the archive containing the Device Monitor Frontend version 7.21 distribution kit. In our example, the file will be extracted to the folder `/tmp/iwdm`:

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.21.0.402.tar.xz
-C /tmp/iwdm
```

5. Go to the folder `/tmp/iwdm` and reset the Platform installation:

```
./setup.py reset
```

6. Restart the current server with the command:

```
reboot
```

7. To free up disk space, you can delete the `/tmp/iwdm` folder.
8. If you are upgrading by switching to another server or to a new OS, copy the folders containing the data that were specified during installation to another partition or to the new server.

> **Note:**
>
> By default, folders are located along the **`/opt`** path.
>
> In **Device Monitor versions below 7.16**, folders were located along the **`/mnt`** path by default.
> Make sure to copy the folders while preserving rights and owners. Use standard tools for copying, such as the **`rsync`** utility.

9. On the central node of the Platform, unpack the archive containing the Device Control version 1.5 distribution kit and run the command:

```
./setup.py reset
```

> **Important!**
>
> Since the server also has Activity Monitor installed, its installation will be reset as a result of resetting the Platform installation. When the installation is reset on the central node, the products on the office nodes will stop working.

10. Restart the current server using the command:

```
reboot
```

11. On the central node of the Platform, install Activity Monitor version 3.6 from its own installation file with the command:

    ```
    ./setup.py install
    ```

    Follow the installation steps from *Activity Monitor. Installation Guide. Installing Activity Monitor*.
    When the installer asks you to specify the folders for storing data, specify the folders containing data from the previous version and select "**n**" when answering the question whether to clear the folders before installation.
12. Then, on the central node of the Platform, install Device Control version 1.5 from its installation file. You can start the installation with a command like:

    ```
    ./setup.py install --dmip=<IP_address_of_Device_Monitor_server>
    ```

    Next, follow the steps to install Device Control.
    You can find the exact command to start the Device Control installation and a description of the next steps in the article *InfoWatch Device Control. Installation Guide. Installing Device Control*.
13. Make sure that the server on which you are updating Device Monitor meets the hardware and software requirements (see Hardware and Software Requirements).
14. Make sure that at least 30 GB of disk space is available in the section with the `/var/lib/containerd` folder.
    To check the available disk space, use the command:

    ```
    df -h /var/lib/containerd
    ```

15. On the Platform office node, go to the folder where the Device Monitor **setup.sh** installation script is located, and run it:

    ```
    ./setup.sh
    ```

    > **Note:**
    >
    > If you encounter a permission error when running the script, make the file executable with the command:
    >
    > ```
    > chmod +x ./setup.sh
    > ```
    >
    > Then run the script.
16. Select **Update**.
17. Select the option for updating with a reset – **Update all after you reset DM Front End: install DM Front End and update DM Server Service**.
    The Platform-based DM Front End component will be installed, and the Device Monitor Server will be updated.
18. Select the Platform installation mode – **Office** (or **Central**, if Device Monitor is installed on the central node).
19. Next, follow the steps for installing the Platform from the article New Installation.
    When the installer asks you to specify the folders for storing data, specify the folders containing data from the previous version and select "**n**" when asked whether to clear the folders before installation.
20. Wait for the DM Front End installation and Device Monitor Server update to complete.
    The following actions will be performed automatically:

- the public key of the **guard** service of the Platform will be retrieved and recorded in Device Monitor; this key is required for the correct interaction between the web interface and the Server;
- the **n.yaml** file will be fixed.

> **Important!**
>
> Any product that will be installed in the Investigation Centre after Device Monitor will generate a new **n.yaml** file, and the section that is required for the correct interaction of the web interface with the Server will be deleted from it. To restore **n.yaml**, follow steps 21a–21c.

21. If you are installing the Platform-based web interface and update the Device Monitor Server separately, using the **DM Front End only** installation and the **DM Server Service only** update options, the actions involving the Platform **guard** service key and the **n.yaml** file from the previous step will not be performed automatically. After installing the Platform and updating the Server, perform them with the installer. To do this:
    a. Run the installation script:
    ```
    ./setup.sh
    ```
    b. Select **Utilities** and run the item **Fix n.yaml file**.
    c. Specify the IP address of the computer on which the Device Monitor Server was installed. If it was installed on the current computer, press **Enter**. Wait for the process to complete.
    d. Run the installation script:
    ```
    ./setup.sh
    ```
    e. Select **Utilities** in the menu and then **Save platform guard public key to IWDM Service**. Wait for the process to complete.
    f. Restart the **iwdms** service:
    ```
    systemctl restart iwdms
    ```
22. Update all installed **Secondary** Device Monitor Servers by performing the following steps on each of them:
    a. Run the script **setup.sh**:
    ```
    ./setup.sh
    ```
    b. Select **Update**.
    c. Select **DM Server Service only**.
    d. Wait for the update process to complete.
23. To display information about the Platform and products in the cluster, run the following command in the directory where the Device Monitor Frontend distribution kit is unpacked:
    ```
    ./setup.py showproducts
    ```
24. If you disabled sending notifications in Telegram before the update, enable it again.

Switching to a Server version with containerization support

To switch to the Device Monitor Server version with containerization support:

1. Delete the old versions of the Platform and Server. See Uninstalling the Web Interface and the Device Monitor Server.

> **Important!**
>
> If you want to reinstall the Server using the old data, do not delete the Database!

2. If you want to switch to another server or a new OS, copy the folders containing the data specified during installation to another partition or a new server.

   Note:

   By default, folders are located along the `/opt` path.

   In **Device Monitor versions below 7.16**, folders were located along the `/mnt` path by default. Make sure to copy the folders while preserving permissions and owners. Use standard tools for copying, such as the `rsync` utility.

3. Install the Device Monitor Server. See New Installation.
   When the installer asks you to specify the folders for storing data, specify the folders containing data from the previous version and select "**n**" when answering the question whether to clear the folders before installation.
   When selecting the installation option, choose **Container (podman)**.
   To install over existing data, specify the existing Database during the installation.

Direct updating the Device Monitor Server (when updating to version 7.21.5 or later)

If you update the distributed installation:

1. Update the central node of the cluster and all products that are installed on this node if they were not previously updated to a supported version.
2. Update the Device Monitor **Primary** Server and Device Monitor Frontend on the officer node.
3. Update Device Monitor **Secondary** Severs.

To update the Device Monitor Server:

1. Perform the steps to prepare the server for the Device Monitor update (see Preparing the Environment, make sure that the dotnet version is relevant).
2. Copy the archive containing the Device Monitor Server distribution to the hard drive.
3. Create a new directory and unpack the contents of the archive into it. In the example, the archive will be unpacked into the directory `/dmsl_distr`:

   ```
   mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.5.402.tar.gz -C /dmsl_distr
   ```

4. Go to the directory created in step 3.
5. Make sure that the server corresponds to the hardware and software requirements (Hardware and Software Requirements).

   Примечание:

   During the update process, the installer will verify that at least 100 GB of disk space is available in the directories specified during installation for:

   - **storing ClickHouse data;**
   - **storing PostgreSQL data;**
   - **storing NATS data;**
   - **data storage.**

   If the directories are located on different disks, the system will check for 100 GB of free space on each of them.

6. Run the Device Monitor Server installer by running the command:

   ```
   ./setup.sh
   ```

   Примечание:

   If an access error occurs when running the script, make the file executable using the command:

```
chmod +x ./setup.sh
```

Then run the script.

7. To update, choose **Update**.
8. Select the option for updating – **Update all (DM Front End, DM Server Service)**.
   The installer will unpack the necessary files and begin the installation.
9. Specify the path for the temporary storage of Traffic Monitor events before they are uploaded to Platform (by default: `/opt/factsldrtmdata`) and click **Enter**.
10. Wait for the installation to complete.
11. Update all installed Device Monitor **Secondary** Servers by following the preceding steps of the instructions for them and selecting the option for updating – **DM Server Service only**.
12. To display information about products in a cluster, go to the directory `/dmsl_distr/data/ui/setup` and run the command:

```
./setup.py showproducts
```

13. To free up disk space, you can delete the directory to which you unpacked the Device Monitor Frontend distributive.
14. After the update process is complete, check the status of Device Monitor server service running the command:

```
systemctl status iwdms
```

Updating Device Monitor Server running the Astra Linux OS (when updating to version 7.21.5 or later)
To update Device Monitor Server from version 7.20 or earlier, installed on the Astra Linux OS, HOST mode:

1. Delete the Device Monitor Server according to the article Uninstalling the Web Interface and the Device Monitor Server, without deleting the Database.
2. Install .NET version 8.0:

```
apt install aspnetcore-runtime-8.0
```

3. Wait for the process to complete and verify that the installation was successfull:

```
dotnet --info
```

4. Install Device Monitor Server version 7.21 according to the article New Installation.
   When the installer asks you to specify the folders for storing data, specify the folders containing data of the previous version and select **n** when asked whether the folders should be cleared before installation.
   When selecting an installation option, specify the **Host** option.
   To install over existing data, specify the existing Database during the installation process.
5. Make sure that the server corresponds to the hardware and software requirements (Hardware and Software Requirements).

> **Примечание:**
>
> **During the update process, the installer will verify that at least 100 GB of disk space is available in the directories specified during installation for:**
>
> - **storing ClickHouse data;**
> - **storing PostgreSQL data;**
> - **storing NATS data;**

- **data storage.**

If the directories are located on different disks, the system will check for 100 GB of free space on each of them.

6. Update Device Monitor Frontend according to Direct updating the Device Monitor Server, using the standard method:
   a. Run the installer:

```
./setup.sh
```

   b. Choose **Update**.
   c. The installer will offer to update Device Monitor Frontend. Choose **Yes**.
   d. The installer will offer to update the Device Monitor Server. Choose **No** and follow the steps from the installation instruction in the New Installation article.
   e. Update the **n.yaml** file and obtain the public key **guard.pem**.

7.2 Updating Device Monitor Agents

You can update Device Monitor Agents:

- On workstations running **Windows** and **Linux family OS**:
  - using the distribution task in the Device Monitor web console (see Primary Distribution and Updating Task);
  - using the distribution policies in the Device Monitor web console (see Distribution Policies);
  - locally on each monitored workstation.

Updating Device Monitor Agents on workstations running **macOS** is not supported. To switch to a new version, you need to uninstall the current version of the Agent and install a later version.
When updating Device Monitor Agents to the new version, follow these steps:

1. Perform the update on a group of no more than 10 computers. Make sure that no errors, performance degradation, or application freezes occur on the computers within 2–3 days.
2. Perform the update on a group of no more than 50 computers. Make sure that no errors, performance degradation, or application freezes occur on the computers within 2–3 days.
3. Perform the update on a group of no more than 500 computers. Make sure that no errors, performance degradation, or application freezes occur on the computers within 2–3 days.
4. Perform the update on a group of no more than 1000 computers. Make sure that no errors, performance degradation, or application freezes occur on the computers within 2–3 days.
5. Perform the update on the remaining computers until the update process is fully completed.

Important!

After the update, you need to restart the Agent's workstation.
Without a restart, the following operations may be performed incorrectly:

- monitoring of the clipboard, cloud storages, removable devices, terminal sessions, network resources, files in applications, FTP, and messengers;
- blocking based on the results of analysis in Traffic Monitor:
  - transfer of web mail, mail via POP, SMTP, IMAP, Outlook protocols, as well as raw HTTP requests (Post, Files);
  - copying to/from removable, network, and terminal devices, via the FTP protocol, to cloud storage;
  - printing.

To locally update the Agents on a Windows workstation to the new version:

1. Delete the old version of the Agent (see Uninstalling Device Monitor Agents);
2. Install the new version of the Agent (see Local Installation of the Agent on a Workstation Running Windows).

To locally update the Agents on a workstation running a Linux family OS to the new version:

1. Complete *Step 1* of the local installation instructions (see Local Installation of the Agent on a Workstation Running a Linux OS).

2. Go to the directory where the archive contents were unpacked.
3. Run the update script with the command:

```
sudo ./upgrade.sh [-g '<Proxy_DN>']
```

where `[-g '<Proxy_DN>']` is the optional parameter for explicitly specifying the DN (Issuer Distinguished Name). Use it if you want to set the DN for the proxy certificate.
`<Proxy_DN>` name must contain the CN (Common Name) field. Fields within the name must be comma-separated.

Note:

The default DN value is: `' CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow'`

If you do not use the **`-g`** parameter or if you specify the default value, the DN in the generated connection certificate will look like:
`CN = IWDMProxy(<machine_uuid>)`
`OU = Infowatch TechDep`
`O = Infowatch`
`L = Moscow`
`ST = RU`
`C = RU`
where `<machine_uuid>` is the workstation identifier created by the Agent.

Note:

To display help, run the command:

```
sudo ./upgrade.sh -h
```

4. Wait for the update to complete. You can check its status with the command:

```
sudo systemctl status "iwdm*"
```

Note:

When updating the Agent on Windows 7 and Windows 2008 R2 Server, take into account that if the **corporate network control component** component was previously installed, it will be deleted during the Agent update. If necessary, you can install this component manually using the command line.

Important!

If the stopped Agent has been updated, it will be launched after the update is complete.
After updating the Agent, make sure to restart the workstation so that the new interception mechanism is used for applications that were launched before the update.

Important!

Agents running version 7.13 and earlier that do not support new policies will not work until they are upgraded to version 7.14 or higher. Configuration updates are not delivered to agents running older versions.

7.3 Updating Configuration on Device Monitor Agents

To transfer additional interception technology settings to the Agents without updating them, use the `AgentConfigurationUploader` utility.

Important!

You can use the utility only to update the configuration of the Telegram messenger control. To use it, update the Agents to version 7.19 or higher (for details, see Updating Device Monitor Agents).

You need to run `AgentConfigurationUploader.dll` in the directory where the Device Monitor server is installed.

To add the configuration to the Agent, run the following command in the terminal:

The command to add the configuration to all Agents

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString
“Server=<Server_name>; Port=<Port>; Database=<Database_name>; User Id=<User_name>;
Password=<Database_password>; “ --ObjectType All --Name <Configuration_name> --
Description “<Description>” --Format <File_format> --ConfigFile “<File_path>”
```

where `<Server_name>` is the name of the server where the DBMS is located,

`<Port>` is the port for configuring interaction between the DBMS and the Server (default: 5432),

`<Database_name>` is the name of the database,

`<User_name>` is the name of the DBMS user,

`<Database_password>` is the DBMS password,

`<Configuration_name>` is the configuration name,

`<Description>` is the description of the changes being made (any textual information),

`<File_format>` is the format of the configuration file,

`<File_path>` is the path to the configuration file. If only the file name is specified, the default path is taken from the directory where the command is executed.

Example command

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString
"Server=localhost; Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --
ObjectType All --Name telegram --Description "configuration" --Format gz --ConfigFile
"D:\\Temp\\tg.gz"
```

The command to add the configuration to a specific Agent

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString
“Server=<Server_name>; Port=<Port>; Database=<Database_name>; User Id=<User_name>;
Password=<Database_password>; “ --ObjectType Workstation --ObjectId
“<Workstation_Id>” --Name <Configuration_name> --Description “<Description>” --Format
<File_format> --ConfigFile “<File_path>”
```

where `<Server_name>` is the name of the server where DBMS is located,

`<Port>` is the port for configuring interaction between the DBMS and the Server (default: 5432),

`<Database_name>` is the name of the database,

`<User_name>` is the name of the DBMS user,

`<Database_password>` is the DBMS password,

`<Workstation_Id>` is the unique identifier for the computer with the Agent. To view it:

1. Go to the section **Groups > Computers**.
2. Open the developer console by pressing **F12**.
3. In it, go to **Network > Response**, with **Fetch/XHR** additionally selected.
4. In the **Name** column, select the workstation.

5. In the **GetWorkstation** request, find the `id` parameter of the required computer and copy its value.

`<Configuration_name>` is the configuration name,

`<Description>` is the description of the changes being made (any textual information),

`<File_format>` is the format of the configuration file,

`<File_path>` is the path to the configuration file. If only the file name is specified, the default path is taken from the directory where the command is executed.

Example command

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString
"Server=localhost; Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --
ObjectType Workstation --ObjectId "C6D169D8-AA30-4090-8E81-2734D27A700B" --Name
telegram --Description "конфигурация" --Format gz --ConfigFile "D:\\Temp\\tg.gz"
```

Note:

The command adds a new configuration if it has not been added before, or updates an existing one.

To delete the configuration, run the following command:

The command to delete the configuration on all Agents

```
dotnet AgentConfigurationUploader.dll remove --DbType PostgreSql --ConnectionString
“Server=<Server_name>; Port=<Port>; Database=<Database_name>; User Id=<User_name>;
Password=<Database_password>; “ --ObjectType All --Name <Configuration_name>
```

where `<Server_name>` is the name of the server where the DBMS is located,

`<Port>` is the port for configuring interaction between the DBMS and the Server (default: 5432),

`<Database_name>` is the name of the database,

`<User_name>` is the name of the DBMS user,

`<Database_password>` is the DBMS password,

`<Configuration_name>` is the configuration name.

Example command

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString
"Server=localhost; Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --
ObjectType All --Name telegram
```

The command to delete the configuration on a specific Agent

```
dotnet AgentConfigurationUploader.dll remove --DbType PostgreSql --ConnectionString
“Server=<Server_name>; Port=<Port>; Database=<Database_name>; User Id=<User_name>;
Password=<Database_password>; “ --ObjectType Workstation --ObjectId
“<Workstation_Id>” --Name <Configuration_name>
```

where `<Server_name>` is the name of the server where the DBMS is located,

`<Port>` is the port for configuring interaction between the DBMS and the Server (default: 5432),

`<Database_name>` is the name of the database,

`<User_name>` is the name of the DBMS user,

`<Database_password>` is the DBMS password,

`<Workstation_Id>` is the unique identifier for the computer with the Agent. To view it:

1. Go to the section **Groups > Computers**.
2. Open the developer console by pressing **F12**.
3. In it, go to **Network > Response**, with **Fetch/XHR** additionally selected.
4. In the **Name** column, select the workstation.
5. In the **GetWorkstation** request, find the `id` parameter of the required computer and copy its value.

`<Configuration_name>` is the configuration name.

Example command

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString
"Server=localhost; Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --
ObjectType Workstation --ObjectId "C6D169D8-AA30-4090-8E81-2734D27A700B" --Name
telegram
```

8 Uninstalling Device Monitor

This section contains the following articles:

1. Deleting the Web Interface and the Device Monitor Server
2. Deleting Device Monitor Agents

8.1 Uninstalling the Web Interface and the Device Monitor Server

To uninstall the Device Monitor web interface:

1. Go to the directory on the server where the distribution archive was unpacked during installation.
2. Unpack the archive containing the Device Monitor Frontend distribution version 7.21:

```
tar xvf data/ui/iw_devicemonitor_setup_7.21.0.310.tar.xz
```

3. Run the command:

```
./setup.py remove
```

4. Wait for the uninstall to complete. The program will uninstall the Device Monitor web interface.

The Device Monitor Server is uninstalled with the *remove.sh* script, which is located in the same directory.

To uninstall the Device Monitor Server:

1. Run the uninstall script as the `root` superuser:

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

> **Note:**
>
> If you encounter a permissions error when running the script, make the file executable by running the command:
>
> ```
> chmod +x ./remove.sh
> ```
>
> Then run the script.

2. Confirm the uninstall request by pressing **Y**.
3. Wait for the server service to stop and for its type to be determined.

```
Stopping the service iwdms...
Service iwdms stopped
Server role: primary
```

4. If the server is the primary one, confirm the subsequent uninstalling of the database. Press **Y** and enter the database user password to confirm the uninstalling.
5. If you need to uninstall the folder with log files (logs), press **Y**.
6. If you need to uninstall the folder of the file queue, press **Y**. If you enter **N**, the folder with shadow copies of events will be preserved, as it may contain events that have not yet been sent to Traffic Monitor or Activity Monitor.
7. Wait for the uninstalling process to complete, which includes:
   - uninstalling the DBMS. If you entered **N** in step 5, the server will be marked as *obsolete*;
   - uninstalling server folders;
   - uninstalling the server service;
   - uninstalling the *iwdms* user;
   - uninstalling the distribution service, if it was installed.
8. During the uninstalling process, errors may occur. For example, in cases where the server was not fully configured, the database was unavailable at the time of uninstalling, or errors occurred when determining the server type. In this case, you will see the error text in the console and be asked whether to continue uninstalling only the Device Monitor server files.

Important!

In case of a distributed installation, if the product is installed on an office node and there are no other products on that node, then after uninstalling the product from the node, we also recommend to uninstall the platform elements. To do this, after running the command `./setup.py remove`, also run the command `./setup.py reset`.

If the product is installed on the central node or if other products are also installed on the office node, we strongly recommend not to run `./setup.py`.

8.2 Uninstalling Device Monitor Agents

This article lists the possible methods for uninstalling the InfoWatch Device Monitor Agent. Agents are uninstalled locally on workstations:

- Local Uninstallation of an Agent on a Workstation Running Windows OS
- Local Uninstallation of an Agent on a Workstation Running a Linux Family OS
- Local Uninstallation of an Agent on a Workstation Running Mac OS

Important!

Turning off the computer's power during the installation/uninstallation of the Agent may lead to errors resulting in unstable operation of the operating system.
If you encounter difficulties while uninstalling the Agent, we recommend contacting the InfoWatch technical support.

8.2.1 Local Uninstallation of an Agent on a Workstation Running Windows OS

This subsection describes the methods for locally uninstalling InfoWatch Device Monitor Agents on workstations running Windows:

- 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 the Agent is not installed in hidden mode, you can uninstall it using the following method:

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 regardless of whether the Agent is in hidden mode or not, but only if an uninstallation password (a password to protect against deletion) is not set.
We recommend using this method when:

- you cannot uninstall the Agent using methods mentioned earlier;
- the Agent and its parts could have remained in the registry and/or on the disk;
- you cannot reinstall the Agent on the workstation.

To uninstall the 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 the Agent.
3. Select **Uninstalling** – **InfoWatch Device Monitor Client**.
4. Wait for the uninstallation to complete and restart the computer.

Uninstalling Agent using Windows Management Instrumentation (WMI)

You can uninstall the Agent using Windows Management Instrumentation (WMI). To do this:

1. Run the command line (`cmd.exe`) as an administrator.
2. Run the Agent uninstallation using one of the following methods, depending on whether an uninstallation password is set:

- If the password is not set, run the command:

```
wmic product where "Name like '%%Device Monitor client%%'" call uninstall
```

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

- If the password is set:
  i. Find out the Agent's identifier by running the command:

```
wmic product where "Name like '%%Device Monitor client%%'" get
IdentifyingNumber
```

  ii. Run the Agent uninstallation command:

```
msiexec /x {<IdentifyingNumber>} /qn /lvp c:\Windows\dm.log
UNINSTALL_PASSWORD=<password>
```

  where `<IdentifyingNumber>` is the Agent identifier;
  "`/qn`" is the parameter that hides the `msiexec` graphical interface. If you want to monitor the uninstallation process, use the "`/q`" parameter instead;
  "`/lvp c:\Windows\dm.log`" is the optional parameter for logging the 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 complete. After that, the log file with the detailed information will be created. In case of successful Agent uninstallation, the log file will contain a record of the following type: *Removal completed with status: 0*.
4. Restart 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 uses the **PsExec** utility and allows you to delete the Agent if the uninstall password is lost:

1. Download the PsExec utility from the official website.
2. Place the downloaded file in the directory `C:\Windows\`
3. Run the command line (`cmd.exe`) as an administrator.
4. Find out the Agent's identifier using the command:

```
wmic product where "Name like '%%Device Monitor client%%'" get
IdentifyingNumber
```

5. Execute the Agent uninstallation command:

```
PsExec.exe -i -s msiexec.exe /X {<IdentifyingNumber>} /q /lvp c:\Windows\dm.log
```

   where `<IdentifyingNumber>` is the Agent identifier;
   "`/q`" is a parameter that runs the command in quiet mode, without user interaction;
   "`/lvp c:\Windows\dm.log`" is the optional parameter for logging the 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 complete. After that, the log file with the detailed information will be created. In case of successful Agent uninstallation, the log file will contain a record of the following type: *Removal completed with status: 0*.
7. Restart the workstation.

8.2.2 Local Uninstallation of an Agent on a Workstation Running a Linux Family OS

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

- Uninstalling with a script
- Uninstalling using OS tools

> **Note:**
>
> Uninstalling Agents on workstations running MOS can be performed using OS only.

Uninstalling with a script

To uninstall the Agent:

1. Make sure that the workstation has an archive containing the package and scripts for installing and uninstalling the Agent. The archive is included in the distribution kit. The name of the archive may vary depending on the OS being used (see Local Installation of the Agent on a Workstation Running a Linux OS.
   If necessary, copy the archive to the workstation and unpack its contents.

   > **Note:**
   >
   > On the workstation, the archive may be located in the directory `/tmp/iwdmupload/`
   >
   > You can also find it on the Device Monitor in the directory `/opt/iw/iwdistribution/bin/SetupPackages`.

2. Go to the directory where the archive contents were unpacked.
3. Run the script:

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

   Example of a command for the Agent on Alt OS:

   ```
   su -c "./remove.sh"
   ```

   As a result, both the Device Monitor Agent and the distribution Agent will be uninstalled.

Uninstalling using OS tools

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

- On Astra Linux:

  ```
  dpkg --purge iwdm
  dpkg --purge iwdeployagent
  ```

- On RED OS and Alt:

  ```
  rpm -e iwdm
  rpm -e iwdeployagent
  ```

- On MOS:

  ```
  rpm -e iwdm
  ```

8.2.3 Local Uninstallation of an Agent on a Workstation Running Mac OS

You can locally uninstall the Agent on a workstation running Mac OS using a script. To do this:

1. Make sure that an archive containing the Agent installation and uninstallation package and scripts is on the workstation. If needed, copy the archive to the workstation and unpack it.

In our example, it is `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. Restart the workstation using the command:

```
reboot
```