

INFOWATCH

InfoWatch Device Control. Руководство по установке

15/09/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования 7

4.1 Типы установки и совместимость с другими продуктами InfoWatch 7

4.1.1 InfoWatch Device Monitor 7

4.1.2 Центр расследований InfoWatch 7

4.2 Типы обновления 9

4.3 Аппаратные требования 9

4.4 Программные требования 10

5 Подготовка сервера 12

5.1 Шаги по подготовке сервера: 12

6 Настройка сетевых правил доступа 17

7 Установка Device Control 18

8 Устранение неполадок 23

9 Обновление Device Control 24

9.1 Варианты обновления Device Control 24

9.2 Прямое обновление Device Control 25

9.3 Обновление Device Control с помощью сброса установки (reset) 28

10 Удаление Device Control 33

Настоящее руководство содержит сведения по установке, обновлению и удалению InfoWatch Device Control (далее также Система или Device Control) – программного обеспечения, позволяющего управлять правами доступа к съемным устройствам.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих установку, обновление, удаление и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем семейств Linux и Microsoft Windows.

2 Комплект документов

В комплект документации по InfoWatch Device Control входят:

- *InfoWatch Device Control. Руководство по установке*. Содержит описание установки, обновления и удаления InfoWatch Device Control.
- *InfoWatch Device Control. Руководство администратора*. Содержит информацию по настройке и подготовке к работе InfoWatch Device Control.
- *InfoWatch Device Control. Руководство пользователя*. Содержит описание работы с InfoWatch Device Control.

Сопутствующая документация по модулю InfoWatch Device Monitor for Linux включает в себя:

- *InfoWatch Device Monitor for Linux. Руководство по установке*. Содержит описание установки, обновления и удаления модуля InfoWatch Device Monitor for Linux.
- *InfoWatch Device Monitor for Linux. Руководство пользователя*. Содержит описание работы с InfoWatch Device Monitor for Linux.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера;
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

4 Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования

4.1 Типы установки и совместимость с другими продуктами InfoWatch

4.1.1 InfoWatch Device Monitor

Для работы **Device Control 1.4** необходим модуль **InfoWatch Device Monitor for Linux 7.20**, установленный с ним в одном кластере. При этом они могут быть установлены как на разных серверах, так и на одном.

> **Примечание:**
>
> Вы можете установить их в любом порядке, но в случае миграции правил рекомендуется устанавливать Device Monitor первым. Подробнее о миграции см. ниже.

Для контроля доступа к внешним устройствам Device Control использует Агенты Device Monitor версии 7.14 и выше.

Миграция правил контроля внешних устройств и белых списков из Device Monitor

С версии Device Monitor for Linux 7.15 работа с правилами контроля внешних устройств осуществляется в Device Control. При миграции сервера Device Monitor for Windows на Device Monitor for Linux 7.20 вы можете перенести старые правила и белые списки в Систему. Для этого:

1. Произведите миграцию Device Monitor на старую базу данных.
   В процессе инсталлятор спросит вас, хотите ли вы перенести правила и белые списки в Device Control. Подробнее см. *InfoWatch Device Monitor for Linux. Руководство по установке. Установка Device Monitor. Новая установка*.
2. Установите Device Control в кластер с Device Monitor.
   Правила контроля внешних устройств и белые списки появятся на вкладке **Правила** раздела **Устройства**. Подробнее см. *InfoWatch Device Control. Руководство пользователя. Вкладка "Правила"*.

4.1.2 Центр расследований InfoWatch

Device Control является частью Центра расследований InfoWatch.

Центр расследований InfoWatch – это единый интерфейс для работы и эффективного взаимодействия следующих продуктов InfoWatch:

- Activity Monitor 3.5
- Data Discovery 2.2
- Data Access Tracker 2.4
- Prediction 3.5
- Vision 3.7

- Device Control 1.4

Каждый продукт может быть установлен и работать отдельно, однако использование нескольких продуктов одновременно существенно повышает возможности офицера по обеспечению информационной безопасности компании.

Основой для установки каждого продукта Центра расследований выступает Платформа. Инсталлятор каждого продукта содержит и Платформу, и продуктовые компоненты. Обе части обязательны к установке при развертывании продуктов.
И продуктовые компоненты, и Платформа поддерживают установку в двух режимах:

- `central`;
- `office`.

Режимы установки продукта и Платформы вы указываете при запуске инсталлятора. Если оба режима не указаны пользователем, инсталлятор по умолчанию использует значение `central` для обоих компонентов.

Центр расследований поддерживает **распределенную установку**: центральная (`central`) и офисные (`office`) ноды Платформы объединены в кластер.
Вы можете установить компоненты продуктов и на центральную, и на офисные ноды Платформы. Это позволяет создать кластер Платформы с несколькими продуктами с учетом инфраструктуры, требований к безопасности и доступных мощностей компании.

Важно!

При распределенной установке примите во внимание следующие ключевые аспекты:

- Продукты в кластере должны быть установлены на одной версии Платформы – в номерах версий должны совпадать первые два числа. Версия центральной ноды Платформы должна быть самой новой в кластере.
- Если вы устанавливаете в кластер продукт на новой версии Платформы, то после этого обновите остальные продукты.
- В одном кластере можно развернуть только одну центральную ноду Платформы и каждый продукт в режиме `central` только в единственном экземпляре.
- Если в кластере уже установлен продукт в режиме `central`, еще одна установка этого продукта в режиме `central` в том же кластере будет прервана ошибкой.
- Device Control и Data Access Tracker поддерживают установку только в режиме `central`. При этом эти продукты поддерживают установку как на центральную, так и на офисные ноды Платформы.

Продукты в одном кластере имеют:

- доступ ко всей функциональности в одной консоли управления;
- общие настройки;
- общую ролевую модель;
- общий доступ к данным независимо от того, на каком из них выполнена интеграция с источником, а также доступ к обработанным данным.

Важно!

Для подключения к веб-интерфейсу Центра расследований **всегда** используйте адрес или имя сервера, на котором установлена **Платформа в режиме** `central`.

Если в распределенной установке продукт в режиме `central` установлен на офисной ноде Платформы, для работы все равно используйте центральную ноду Платформы (`central`).

Продукты Центра расследований InfoWatch поддерживают совместную установку на одном сервере.

Вы можете установить **Device Control 1.4 совместно** с:

- **Activity Monitor 3.5**
- **Data Discovery 2.2**
- **Data Access Tracker 2.4**
- **Prediction 3.5**
- **Vision 3.7**
- **Data Analysis Service 1.6**

Примечание:

Для расчета аппаратных требований при совместной установке **учитывайте требования каждого продукта**. Для расчета требований под конкретный проект обратитесь к специалистам компании InfoWatch.

Подробнее о процессе установки см. *Установка Device Control*.

4.2 Типы обновления

Device Control поддерживает:

- прямое обновление;
- обновление с помощью сброса и переустановки на старые данные.

Подробнее о процессе обновления см. *Обновление Device Control*.

4.3 Аппаратные требования

Минимальные требования, необходимые для установки Системы:

- Количество ядер процессора: 4 (частота - 3.1 ГГц, разрядность - 64 бит, с поддержкой инструкций SSE 4.2);
- ОЗУ: 20 ГБ;
- Жесткий диск: 101 ГБ.

Нагрузка на аппаратное обеспечение рассчитывается, исходя из объема анализируемых данных. В таблице приведены системные требования к процессору, объему оперативной памяти и жесткого диска для установки и работы Device Control на отдельном сервере.

Количество сотрудников	Срок хранения в архиве	Ядер/потоков (ядер в VM)	ОЗУ, ГБ	Жесткий диск, ГБ
100	Хранение – 1 год	4/8 (8)	20	101
200		4/8 (8)	20	137

Количество сотрудников	Срок хранения в архиве	Ядер/потоков (ядер в VM)	ОЗУ, ГБ	Жесткий диск, ГБ
500		4/8 (8)	20	247
1000		8/16 (16)	32	430
3000		12/24 (24)	48	1164
6000		16/32 (32)	64	2264
10000		24/48 (48)	80	3764

4.4 Программные требования

Для установки и работы в Системе может быть использовано следующее программное обеспечение:

Тип ПО	Варианты
Операционная система	• Astra Linux Special Edition, версии: • 1.7 в редакции "Воронеж" • 1.7.5 в редакциях "Орел" и "Смоленск" • 1.8 в редакциях "Орел", "Воронеж" и "Смоленск" • Red Hat Enterprise Linux, версии: • 7.9 • 8.9 • 8.10 • Oracle Linux, версии: • 7.9 • 8.4 • 8.10 • РЕД ОС, версии: • 7.3.3 • 8 • ОС Альт Сервер 10.2 • МОС ОС Арбат версии 15.5 **Важно!** Модули **netfilter** и **nat** должны быть обязательно загружены в ядро ОС
Браузер	• Google Chrome; • Яндекс.Браузер. **Важно!** Для корректной работы рекомендуется использовать последние версии поддерживаемых браузеров

Примечание:

Device Control использует PostgreSQL 16.4. СУБД поставляется вместе с продуктом и не требует отдельной установки.

5 Подготовка сервера

Перед установкой Device Control выполните шаги по подготовке сервера.

5.1 Шаги по подготовке сервера:

1. **На сервере под управлением МОС ОС:**

   Убедитесь, что доступны официальные репозитории ОС:

   - `software`
   - `update`
   - `oss`
2. Установите интерпретатор языка Python версии 2.7. Он необходим для установки Системы, так как программа установки написана на языке Python версии 2.7.

   > **Примечание:**
   >
   > Пакет с интерпретатором не входит в состав дистрибутива Device Control.

3. Настройте правила POD сети или отключите межсетевой экран (подробнее см. статьи Базы знаний *Конфликты при взаимодействии firewalld и Kubernetes*, *Полное отключение межсетевого экрана*).
4. Если вы используете распределенную структуру, убедитесь, что:
   - **на всех нодах кластера** открыт UDP-порт 8472 или выполните команду:

     ```
     firewall-cmd --zone=public --add-port=8472/udp
     ```

   - **на ноде, где будет установлен Device Control**, открыт TCP-порт 6443 или выполните команду:

     ```
     firewall-cmd --zone=public --add-port=6443/tcp
     ```

5. Для корректной работы Device Control настройте сетевые правила доступа (подробнее см. *Настройка сетевых правил доступа*).
6. Device Control использует компонент Kubernetes. Для корректной установки Системы и работы Kubernetes на сервере должны быть установлены следующие пакеты:
   - **conntrack** или **conntrack-tools** (пакет необходимо установить, даже если **libnetfilter_conntrack** уже установлен).
     Убедитесь, что пакет установлен. Для этого введите в командной строке:

     ```
     conntrack
     ```

     В результате будут выведены сведения о работе с **conntrack** и его установленная версия.

```
Command line interface for the connection tracking system. Version 1.4.4
Usage: conntrack [commands] [options]

Commands:
  -L [table] [options]          List conntrack or expectation table
  -G [table] parameters         Get conntrack or expectation
  -D [table] parameters         Delete conntrack or expectation
  -I [table] parameters         Create a conntrack or expectation
  -U [table] parameters         Update a conntrack
  -E [table] [options]          Show events
  -F [table]                    Flush table
  -C [table]                    Show counter
  -S                            Show statistics

Tables: conntrack, expect, dying, unconfirmed

Conntrack parameters and options:
  -n, --src-nat ip                      source NAT ip
  -g, --dst-nat ip                      destination NAT ip
  -j, --any-nat ip                      source or destination NAT ip
  -m, --mark mark                       Set mark
  -c, --secmark secmark                 Set selinux secmark
  -e, --event-mask eventmask            Event mask, eg. NEW,DESTROY
  -z, --zero                            Zero counters while listing
  -o, --output type[,...]               Output format, eg. xml
  -l, --label label[,...]               conntrack labels

Expectation parameters and options:
  --tuple-src ip        Source address in expect tuple
  --tuple-dst ip        Destination address in expect tuple

Updating parameters and options:
  --label-add label     Add label
  --label-del label     Delete label

Common parameters and options:
  -s, --src, --orig-src ip              Source address from original direction
  -d, --dst, --orig-dst ip              Destination address from original direct
ion
  -r, --reply-src ip            Source addres from reply direction
  -q, --reply-dst ip            Destination address from reply direction
  -p, --protonum proto          Layer 4 Protocol, eg. 'tcp'
  -f, --family proto            Layer 3 Protocol, eg. 'ipv6'
  -t, --timeout timeout         Set timeout
  -u, --status status           Set status, eg. ASSURED
  -w, --zone value              Set conntrack zone
  --orig-zone value             Set zone for original direction
  --reply-zone value            Set zone for reply direction
  -b, --buffer-size             Netlink socket buffer size
  --mask-src ip                 Source mask address
  --mask-dst ip                 Destination mask address
```

Если пакет не установлен, установите его с помощью команды:

- **для Red Hat Enterprise Linux, Oracle Linux и РЕД ОС**

```
yum install conntrack
```

- **для ОС Astra Linux**

```
apt-get install conntrack
```

- **для ОС Альт**

```
apt-get install conntrack-tools
```

- **для МОС ОС**

```
zypper install conntrack-tools
```

Если пакет недоступен в репозитории, скачайте его самостоятельно, например, из официального репозитория РЕД ОС. Затем перейдите в директорию с пакетом и установите его вручную с помощью команды вида:

- **для Red Hat Enterprise Linux, Oracle Linux, РЕД ОС и ОС Альт**

```
rpm -Uhv ./<имя_пакета>
```

- **для ОС Astra Linux**

```
dpkg -i ./<имя_пакета>
```

- **для МОС ОС**

```
zypper install <имя_пакета>
```

- **socat** – аналогично пакету **conntrack**.

7. Если вы используете антивирус, настройте его для совместной работы с Системой (см. статью Базы знаний *Настройка антивируса для продуктов Платформы*).
8. **На сервере под управлением МОС ОС:**

   Установите пакеты `ethtool`, `app_armor` и `sysctl` с зависимостями:

```
zypper install ethtool
zypper install patterns-base-apparmor
zypper install procps
zypper install libprocps7
```

9. **На сервере под управлением Red Hat Enterprise Linux и РЕД ОС настройте SELinux.**

   Для корректной работы используемого `containerd` **обновите** политики SELinux или **отключите** систему контроля доступа:

   - **Чтобы обновить политики SELinux**, скачайте и установите пакет `container-selinux`.
     Вы можете сделать это, выполнив команду:

```
yum install container-selinux
```

     > **Примечание:**
     >
     > Пакет не входит в состав дистрибутива продукта.
     >
     > Пакет может отсутствовать в репозиториях. В этом случае загрузите и установите его вручную.

   - **Чтобы отключить SELinux**:
     a. Выполните команды от имени суперпользователя `root`:

```
setenforce 0
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
```

b. Перезагрузите сервер с помощью команды:

```
reboot
```

c. Проверьте статус системы SELinux с помощью команды:

```
sestatus
```

10. **На сервере под управлением ОС Альт:**

    Установите пакеты:

    - **python-modules-json**;
    - **python-modules-distutils**;
    - **python-modules-sqlite3**.

    > **Примечание:**
    >
    > Пакеты не входят в состав дистрибутива Device Control.
    >
    > Пакеты могут отсутствовать в репозиториях некоторых операционных систем. В этом случае загрузите и установите требуемые пакеты вручную.

11. **На сервере под управлением ОС Astra Linux Special Edition:**

    Отключите настройку *astra-nochmodx-lock*. Для этого выполните команду:

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

12. Убедитесь, что на сервере установлены актуальные дата и время.

Дистрибутив Device Control представляет собой архив `iw_devicecontrol_setup_1.4.X.xxx.tar.xz`, где xxx — номер сборки. Архив содержит набор бинарных модулей образов контейнеров, необходимых для развертывания Device Control без доступа к сети Интернет. Архив также содержит программу установки.

Вы можете установить Device Control:

- на сервере совместно с другими продуктами;
- в кластере с другими продуктами.

> **Важно!**
>
> Device Control должен быть установлен в одном кластере с Device Monitor.
>
> Вы можете установить в кластере только один экземпляр Device Control и только в режиме `central`.

Важно!

Если вы устанавливаете Device Control в одном кластере с другими продуктами InfoWatch, то убедитесь, что версия Платформы совпадает у всех продуктов. В противном случае продукты, установленные на старой версии Платформы, необходимо обновить.

Чтобы узнать версию Платформы устанавливаемого продукта:

1. Распакуйте архив с дистрибутивом Device Control. Для этого перейдите в директорию с архивом и выполните команду:

   ```
   tar xvf iw_devicecontrol_setup_1.4.X.xxx.tar.xz
   ```

2. Выполните команду:

   ```
   cat platform/setup.yaml | grep version
   ```

Важно!

Необходимо, чтобы все ноды кластера были доступны друг для друга в сети. Для этого должны быть открыты необходимые порты (см. *Настройка сетевых правил доступа*).
Также перед установкой убедитесь, что:

- настроено разрешение имен нод средствами DNS
  или
- в файле `/etc/hosts` каждой ноды определено соответствие между адресами и именами нод.

Для проверки доступности нод выполните команду между нодами кластера:

```
ping <имя ноды>
```

Для установки Device Control используйте командную строку.

6 Настройка сетевых правил доступа

Для корректной работы Device Control должны быть разрешены соединения:

Соединение	Порт	Описание
Рабочая станция Администратора → Сервер Device Control	TCP 22	Используется для управления сервером Device Control через SSH-консоль
Рабочая станция Офицера Безопасности → Центр расследований	TCP 443	Используется для доступа Офицера безопасности к веб-интерфейсу Центра расследований (центральная нода платформы).
Сервер Device Control → Сервер Device Monitor	TCP 15007	Доступ к API Device Monitor
Сервер Device Monitor → Сервер Device Control	TCP 17104	Взаимодействие сервера Device Monitor с сервером Device Control

7 Установка Device Control

> **Примечание:**
>
> Если вы устанавливаете Device Control на сервер, на котором уже установлен модуль InfoWatch Device Monitor, инсталлятор не запросит часть параметров, так как эти директории и настройки уже были указаны при первичной установке Платформы.

Чтобы установить Device Control:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям (см. *Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования*).

   > **Примечание:**
   >
   > В ходе установки инсталлятор проверит наличие:
   >
   > - не менее 100 ГБ на диске для директорий размещения данных ClickHouse, PostgreSQL, NATS и бинарных данных. Эти директории необходимо указать при выполнении инструкций по установке. Если директории находятся на разных дисках, то проверятся наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 8 ГБ ОЗУ;
   > - не менее 2 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета `conntrack.`

2. Выполните шаги по подготовке сервера к установке Device Control (см. *Подготовка сервера*).
3. Создайте новую директорию на диске, например, `devicecontrol`:

   ```
   mkdir devicecontrol
   ```

4. Скопируйте архив **iw_devicecontrol_setup_1.4.X.xxx.tar.xz** в созданную директорию.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом Device Control в созданную директорию:

   ```
   tar xvf iw_devicecontrol_setup_1.4.X.xxx.tar.xz
   ```

7. Если вы хотите установить Device Control на офисной ноде, но Платформа еще не установлена на сервере, то установите ее. Для этого:
   a. Перейдите в директорию `platform`:

      ```
      cd platform
      ```

   b. Запустите программу установку Платформы с помощью команды:

```
./setup.py install --nodemode=office
```

c. Выполните шаги установки Платформы 13-22 данной инструкции.
При дальнейшей установке Системы эти шаги будут пропущены.
d. Вернитесь в директорию с инсталлятором Device Control:

```
cd ..
```

8. Если вы устанавливаете Device Control на офисной ноде Платформы, выполните следующую команду, указав в ней IP адрес центральной ноды:

```
scp root@<IP_адрес_центральной_ноды>:/etc/kubernetes/admin.conf $HOME/.kube/config
```

9. Запустите программу установки с помощью команды вида:

```
./setup.py install --nodemode=<режим_установки_Платформы> --productmode=central --
dmip=<IP_адрес_сервера_Device_Monitor>
```

Примечание:

Чтобы установить:

- **на центральную ноду Платформы продукт в режиме central:**

```
./setup.py install --nodemode=central --productmode=central --
dmip=<IP_адрес_сервера_Device_Monitor>
```

- **на офисную ноду Платформы продукт в режиме central:**

```
./setup.py install --nodemode=office --productmode=central --
dmip=<IP_адрес_сервера_Device_Monitor>
```

Если вы не укажете режимы установки Платформы и продукта, инсталлятор по умолчанию выберет режим `central`.

Если вы не укажете IP адрес сервера Device Monitor, то инсталлятор по умолчанию использует IP адрес текущего сервера.

Важно!

Во время установки могут быть недоступны продукты Платформы, установленные на сервере.

10. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.

11. Введите "**y**", чтобы принять лицензионное соглашение и нажмите **Enter**.

    > **Примечание:**
    >
    > Если отклонить лицензионное соглашение, инсталлятор прервет процесс и завершит работу.

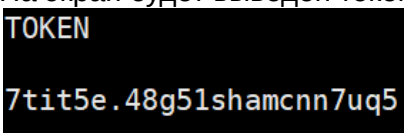
12. Если вы устанавливаете **центральную ноду Платформы** (`--nodemode=central`), введите IP-адрес сетевого интерфейса для взаимодействия с кластером в формате IPv4: "xxx.xxx.xxx.xxx" (по умолчанию: `0.0.0.0`) и нажмите **Enter**.
    Если указать `0.0.0.0` , будут использованы все доступные сетевые интерфейсы.

    > **Примечание:**
    >
    > Здесь и далее для использования значений, предложенных по умолчанию, нажмите **Enter** без ввода значений.

13. Если вы устанавливаете **офисную ноду Платформы** (`--nodemode=office`):
    a. Укажите адрес центральной ноды Платформы в формате IP-адреса или доменного имени (например: `192.0.2.0` или `host.example.com`).
    b. Укажите токен для подключения к центральной ноде Платформы.
    Чтобы получить токен для подключения к центральной ноде Платформы:
        i. Подключитесь по ssh к консоли центральной ноды Платформы;
        ii. Выполните в терминале команду для получения токена:

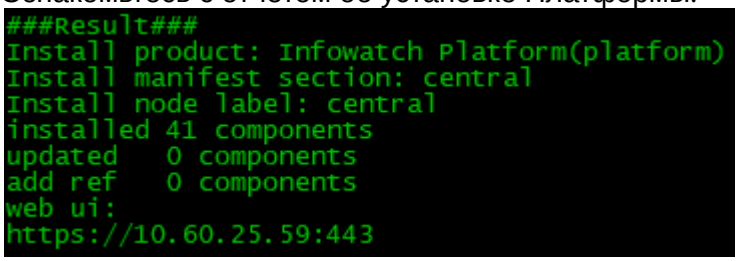
        ```
        kubeadm token list
        ```

        На экран будет выведен токен:

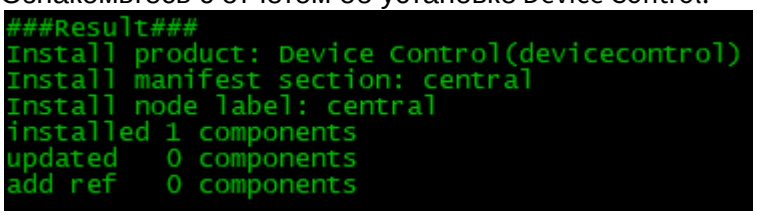
        

        Токен в нашем примере: `7tit5e.48g51shamcnn7uq5`
        iii. Укажите лейбл ноды (по умолчанию: `office`) и нажмите **Enter**.
        Лейбл может состоять из букв латинского алфавита и/или цифр. Длина лейбла не должна превышать 32 символа.
14. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
15. Укажите путь для размещения данных Clickhouse (по умолчанию `/opt/chdata`) и нажмите **Enter**.
16. Укажите путь для размещения данных PostgreSQL (по умолчанию `/opt/pgdata`) и нажмите **Enter**.
17. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
18. Укажите путь для хранения данных (по умолчанию `/opt/dsdata`) и нажмите **Enter**.
19. Укажите путь для временного хранения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.
20. Если вы устанавливаете **центральную ноду Платформы**, укажите порт подключения к веб-интерфейсу (по умолчанию: `443`) и нажмите **Enter**.

21. Дождитесь завершения установки Платформы.
22. Ознакомьтесь с отчетом об установке Платформы.



    При установке центральной ноды Платформы в графе **`web ui`** указаны адрес и порт для подключения к веб-интерфейсу (в нашем примере – `https://10.60.25.59:443`).
23. Дождитесь окончания процесса установки. Программа установит компоненты Device Control и требуемое окружение.
24. Ознакомьтесь с отчетом об установке Device Control:



25. Если вы установили Device Control на офисной ноде Платформы, выполните команду копирования конфигурационного файла:

    ```
    cp -f /etc/kubernetes/kubelet.conf $HOME/.kube/config
    ```

    Если будет предложено копировать с заменой, согласитесь, нажав **Enter**.
26. Убедитесь, что сервисы запустились, выполнив команду.

    ```
    kubectl get pods -n infowatch
    ```

    Каждый сервис должен иметь статус `Running`.
27. Чтобы вывести на экран информацию о Платформе, выполните команду:

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

    Вывод команды должен содержать строку **`DbState: commited`**. Например:

    ```
    platform Title: Infowatch Platform Version: 2.5.1.363 Node: my-server(central) Mode:
    central DbState: commited
    ```

28. Если Device Monitor был установлен до Device Control, обновите конфигурационный файл `n.yaml`:
    a. На сервере, где установлен Device Monitor, перейдите в директорию, куда был распакован дистрибутив Device Monitor.
    b. Запустите скрипт **setup.sh**, выполнив команду:

```
./setup.sh
```

c. Выберите в меню пункт **Utilities**.
d. Выберите **Fix n.yaml file**.
e. Введите IP-адрес сервера Device Monitor и дождитесь окончания процесса.

> **Важно!**
>
> После добавления в кластер любого продукта Центра Расследования, необходимо выполнять шаг 27.

Чтобы начать работу в Device Control:

1. Установите Device Monitor, если он еще не установлен. Подробнее см. *InfoWatch Device Monitor for Linux. Руководство по установке*.
2. Настройте передачу событий из Device Monitor в Платформу, см. *InfoWatch Device Monitor for Linux. Руководство пользователя. Настройка Device Monitor. Серверы Device Monitor*.
3. В базе данных Device Monitor включите настройку для отправки событий контроля устройств в Платформу. Вы можете это сделать, например, с помощью следующей команды:

```
UPDATE public."Settings" SET "Value"='True' WHERE "Name"='SEND_DEVICE_EVT_TO_PLATFORM';
```

4. Убедитесь, что в Device Monitor в разделе **Настройки** → **Настройки продукта** → **Агенты** для настройки **Логировать события от перехватчика устройств и облачных хранилищ** выбрано значение **Логировать всегда**. Подробнее см. *InfoWatch Device Monitor for Linux. Руководство пользователя. Настройка Device Monitor. Агенты*.
5. Подключитесь к веб-интерфейсу Центра расследований. Для этого введите в браузере адрес и порт центральной ноды Платформы.
   Если веб-консоль уже была открыта до установки Системы, то достаточно обновить страницу в браузере.

Чтобы после установки изменить IP адрес сервера Device Monitor, с которым будет взаимодействовать Device Control:

1. Выполните следующую команду, где вместо `xxx.xxx.xxx.xxx` укажите адрес сервера Device Monitor:

```
kubectl -n infowatch patch endpoints dm-external --type='merge' -p '{"subsets":
[{"addresses":[{"ip":"xxx.xxx.xxx.xxx"}],"ports":[{"port":15007,"protocol":"TCP"}]}]}'
```

2. Убедитесь, что указан нужный вам адрес. Для этого выведите текущее значение:

```
kubectl -n infowatch get endpoints dm-external -o wide
```

8 Устранение неполадок

Во время установки Системы возможны сбои: прерывания работы программы установки, отключение электричества и т.д. В этом случае Система будет установлена некорректно. Для решения этой проблемы, а также при обновлении на новую версию с удалением старой версии, следует сбросить установку. После сброса все данные сохранятся в Системе, а установку необходимо произвести заново (см. *Установка Device Control*). В процессе установки на вопрос об удалении существующих данных выберите ответ **Нет**.

Чтобы сбросить установку:

1. Если Device Control и Prediction установлены совместно, остановите расчет данных Prediction перед сбросом установки Device Control (подробнее см. *Обязательные действия для обновления продуктов на Платформе, которые установлены совместно с Prediction*).
2. Запомните или сохраните пути к текущим директориям хранения данных. Получить список директорий можно, выполнив команду:

   ```
   cat /var/lib/iwplatform/data/volumes.txt
   ```

3. Запомните или сохраните лейблы нод. Чтобы посмотреть список лейблов в кластере, выполните команду:

   ```
   kubectl get node -n infowatch -o jsonpath="{range .items[*]}
   {.metadata.annotations.flannel\.alpha\.coreos\.com/public\-ip}
   {.metadata.labels.kubernetes\.io/hostname} {.metadata.labels.iwnode}{'\n'}{end}"
   ```

4. Если неполадки возникли в процессе установки, то перейдите в директорию, где распакован дистрибутив продукта. В ином случае, если осуществляется обновление Системы, перейдите в директорию, где установлена Система.
5. Выполните команду:

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

6. После сброса при установке присвойте нодам кластера те же лейблы, которые были до начала процедуры сброса.

Важно!

При сбросе установки Системы автоматически производится сброс всех других продуктов Платформы, установленных на сервере.

Если произведен сброс установки на центральной ноде Платформы, станут недоступны компоненты всех продуктов в кластере. В этом случае выполните сброс на каждой офисной ноде.

После установки Device Control повторно установите и другие продукты в кластере.

9 Обновление Device Control

Обновление Device Control производится вручную, с помощью командной строки.

Для обновления Системы используется архив `iw_devicecontrol_setup_x.x.x.xx.tar.xz`, где x.x.x.xx – номер версии. Архив входит в состав дистрибутива. Архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Системы без доступа к сети Интернет.

9.1 Варианты обновления Device Control

Важно!

В случае совместной установки Device Control с Prediction, необходимо остановить расчет данных Prediction на время обновления Device Control. Подробнее см. *InfoWatch Prediction. Руководство по установке. Прямое обновление Prediction или Обновление Prediction с помощью сброса установки.*

Device Control 1.4 поддерживает:

- прямое стандартное обновление с версий 1.3.x и 1.4.x;
- обновление с помощью сброса текущей установки и переустановки на старые данные.

На время обновления Система будет недоступна во всем кластере. Если до обновления Device Control и другие продукты были установлены в разных кластерах, то объединение их в общий кластер после обновления не поддерживается.

Важно!

Если вместе с Device Control вы планируете обновлять модуль Device Monitor, обновите Device Monitor первым.

Важно!

Если вы обновляете Device Control в одном кластере с другими продуктами InfoWatch, то убедитесь, что версия Платформы совпадает у всех продуктов. В противном случае продукты, установленные на старой версии Платформы, необходимо обновить.

Чтобы узнать версию Платформы обновляемого продукта:

1. Распакуйте архив с дистрибутивом Device Control. Для этого перейдите в директорию с архивом и выполните команду:

   Пример для версии 1.4.0.45:

   ```
   tar xvf iw_devicecontrol_setup_1.4.0.45.tar.xz
   ```

2. Выполните команду:

```
cat platform/setup.yaml | grep version
```

9.2 Прямое обновление Device Control

Важно!

С версии Device Control 1.3 изменился механизм синхронизации правил с Device Monitor. Перед обновлением рекомендуется сделать резервную копию базы данных Device Monitor.

Важно!

После обновления Device Control до версии 1.4, в сохраненных фильтрах будут отсутствовать значения фильтров *Вердикт*, *Тип устройства* и *Идентификатор устройства* (вкладка **События использования**). При необходимости запомните их и установите заново после обновления.

Важно!

Чтобы **обновить распределенный кластер** продуктов Платформы:

1. **Обновите центральную ноду** кластера и все установленные на ней продукты.
2. **Обновите офисные ноды** и все установленные на них продукты.

Прямое обновление поддерживается с версий 1.3.x и 1.4.x.

Чтобы обновить Device Control:

1. Выполните шаги по подготовке сервера к обновлению (см. *Подготовка сервера*).

   Примечание:

   В ходе обновления инсталлятор проверит наличие:

   - не менее 100 ГБ на диске для директорий размещения данных ClickHouse, PostgreSQL, NATS и бинарных данных. Если директории для хранения данных находятся на разных дисках, то проверяется наличие 100 ГБ свободного места на каждом из них;
   - не менее 20 ГБ на диске для директорий с образами;
   - не менее 8 ГБ ОЗУ;
   - не менее 2 ядер процессора;
   - поддержки инструкции SSE 4.2;
   - установленного пакета `conntrack.`

2. Создайте новую директорию на диске (например, `DC`):

```
mkdir DC
```

3. Скопируйте архив **`iw_devicecontrol_setup_1.4.x.xx.tar.xz`** в созданную директорию.
   В нашем примере будет использована версия `1.4.0.45`, ей соответствует архив `iw_devicecontrol_setup_1.4.0.45.tar.xz`.
4. Перейдите в директорию, в которую был скопирован архив.
5. Распакуйте архив с дистрибутивом Device Control в эту директорию:

```
tar -xvf iw_devicecontrol_setup_1.4.0.45.tar.xz
```

6. Убедитесь, что в разделе с директорией `/var/lib/containerd` доступно не менее 50 ГБ дискового пространства.
   Чтобы проверить доступное дисковое пространство, используйте команду:

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

> **Примечание:**
>
> Чтобы освободить дисковое пространство, вы можете удалить образы неиспользуемых контейнеров предыдущих версий. Для этого выполните следующие шаги:
>
> a. Добавьте в файл `/etc/crictl.yaml` (при необходимости создайте его) строки:
>
> ```
> runtime-endpoint: unix:///run/containerd/containerd.sock
> image-endpoint: unix:///run/containerd/containerd.sock
> timeout: 5
> pull-image-on-create: false
> disable-pull-on-run: false
> ```
>
> b. Выполните команды:
>
> i. Для удаления контейнеров Платформы (где x.x.x.x – установленная версия Платформы):
>
> ```
> crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x|latest/ && $1 ~ /
> docker.infowatch.ru\/platform-core-release/ && $1 !~ /flannel/) {print
> $3}')
> ```
>
> ii. Для удаления контейнеров Device Control (где x.x.x.x – установленная версия Device Control):
>
> ```
> crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x/ && $1 ~ /
> docker.infowatch.ru\/devicecontrol/) {print $3}')
> ```

Данные команды удаляют контейнеры всех версий кроме указанной. Не удаляйте контейнеры установленной версии Device Control и Платформы!

7. Если вы обновляете Device Control на офисной ноде Платформы, выполните следующую команду, указав в ней IP адрес центральной ноды:

```
scp root@<IP_адрес_центральной_ноды>:/etc/kubernetes/admin.conf $HOME/.kube/config
```

8. Запустите программу обновления Системы:

```
./setup.py update --dmip=<IP_адрес_сервера_Device_Monitor>
```

Если вы не укажете IP адрес сервера Device Monitor, то инсталлятор по умолчанию использует IP адрес текущего сервера. О том, как изменить этот параметр после обновления, см. *Установка Device Control*.

Важно!

Во время обновления продукты Платформы, уже установленные на сервере, могут быть недоступны.

9. Дождитесь окончания процесса обновления Device Control.
10. Ознакомьтесь с отчетом об обновлении Системы:



11. Если вы обновили Device Control на офисной ноде Платформы, выполните команду:

```
cp -f /etc/kubernetes/kubelet.conf $HOME/.kube/config
```

12. Чтобы вывести на экран информацию об установленных продуктах, выполните команду:

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

13. Чтобы проверить, что обновление прошло успешно, выполните команду:

```
kubectl get pods -n infowatch
```

Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.

14. Обновите конфигурационный файл `n.yaml`:
    a. На сервере, где установлен Device Monitor, перейдите в директорию, куда был распакован дистрибутив Device Monitor.

b. Запустите скрипт **setup.sh**, выполнив команду:

```
./setup.sh
```

c. Выберите в меню пункт **Utilities**.
d. Выберите **Fix n.yaml file**.
e. Введите IP-адрес Сервера Device Monitor и дождитесь окончания процесса.

15. Если на сервере установлены продукты Платформы, обновите их до версий, совместимых с Device Control (см. *Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования*), а затем повторите шаг 14 данной инструкции.
16. Если Device Control установлен в распределенном кластере, обновите Платформу и продукты на других серверах кластера до версий, совместимых с Device Control.
17. Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры аналогично п.6.
18. Очистите кеш браузера, в котором работали до обновления продукта. Веб-интерфейс Центра расследований доступен по адресу центральной ноды Платформы.

9.3 Обновление Device Control с помощью сброса установки (reset)

Важно!

С версии Device Control 1.3 изменился механизм синхронизации правил с Device Monitor. Перед обновлением рекомендуется сделать резервную копию базы данных Device Monitor.

Важно!

После обновления Device Control до версии 1.4, в сохраненных фильтрах будут отсутствовать значения фильтров *Вердикт*, *Тип устройства* и *Идентификатор устройства* (вкладка **События использования**). При необходимости запомните их и установите заново после обновления.

Важно!

Чтобы обновить весь распределенный кластер продуктов на Платформе с помощью сброса (reset) установки, действуйте в следующей последовательности:

1. Выполните **сброс на офисных** нодах с продуктами в режиме `office`.
2. Выполните **сброс на офисных** нодах с продуктами в режиме `central`.
3. Выполните **сброс центральной** ноды.
4. **Установите центральную** ноду кластера.
5. **Установите офисные** ноды с продуктами в режиме `central`.
6. **Установите офисные** ноды с продуктами в режиме `office`.

В рамках обновления кластера выполняйте сброс установки только один раз для каждой ноды.

Обновление с помощью сброса установки состоит из следующих шагов:

1. Сброс установки **с помощью нового инсталлятора**. При сбросе данные Системы не будут удалены.
2. Установка новых версий Платформы и продукта с указанием уже имеющихся папок с данными.

> **Примечание:**
>
> Если вы используете удаленное подключение по протоколу SSH, чтобы избежать проблем в случае разрыва соединения с сервером, рекомендуем использовать утилиту Screen. При отключении от утилиты запущенные в ней процессы не прервутся, что позволит безопасно продолжить обновление.

Чтобы обновить Device Control:

1. Выполните шаги по подготовке сервера к установке Device Control (см. *Подготовка сервера*).

   > **Примечание:**
   >
   > В ходе обновления инсталлятор проверит наличие:
   >
   > - не менее 100 ГБ на диске для директорий размещения данных ClickHouse, PostgreSQL, NATS и бинарных данных. Если директории для хранения данных находятся на разных дисках, то проверяется наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 8 ГБ ОЗУ;
   > - не менее 2 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета `conntrack.`

2. Создайте новую директорию на сервере (например, `devicecontrol`):

   ```
   mkdir devicecontrol
   ```

3. Скопируйте архив `iw_devicecontrol_setup_1.4.X.xxx.tar.xz` в созданную директорию. В нашем примере будет использована версия `1.4.0.45`, соответственно, архив – `iw_devicecontrol_setup _1.4.0.45.tar.xz`.
4. Перейдите в директорию, в которую был скопирован архив.
5. Распакуйте архив с дистрибутивом в эту директорию:

   ```
   tar -xvf iw_devicecontrol_setup_1.4.0.45.tar.xz
   ```

6. После сброса при установке новой версии присвойте нодам кластера те же лейблы, которые были до обновления.

7. Чтобы посмотреть список лейблов в кластере, выполните команду:

```
kubectl get node -n infowatch -o jsonpath="{range .items[*]}
{.metadata.annotations.flannel\.alpha\.coreos\.com/public\-ip}
{.metadata.labels.kubernetes\.io/hostname} {.metadata.labels.iwnode}{'\n'}{end}"
```

8. До сброса установки запомните или сохраните пути к текущим директориям хранения данных. Получить список директорий можно, выполнив команду:

```
cat /var/lib/iwplatform/data/volumes.txt
```

9. Выполните **сброс** текущей установки **с помощью инсталлятора новой версии**:

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

> **Важно!**
>
> Если на сервере установлены другие продукты Платформы, установки этих продуктов будут сброшены в результате сброса установки Платформы. При сбросе установки на центральной ноде продукты на офисных нодах перестанут функционировать.
>
> После установки новой версии Device Control повторно установите продукты Платформы, указав директории с имеющимися данными.
>
> Если на этом сервере вы **уже обновили другой продукт** до совместимой версии, **не выполняйте повторный сброс** при обновлении Device Control, так как требуемая версия Платформы уже установлена.
>
> Если продукт установлен **на офисной ноде в режиме central**, после сброса установки у добавленных ролей пользователя будет **сброшен доступ к продуктам**.

10. Дождитесь окончания процесса сброса установки Платформы и продукта.
11. Перезагрузите сервер с помощью команды:

```
reboot
```

12. Если вы обновляетесь с переходом на другой сервер или на новую ОС, скопируйте на другой раздел или на новый сервер директории с данными, которые были указаны при установке.

> **Примечание:**
>
> В **Device Control 1.0** директории по умолчанию были расположены по пути **`/mnt`**.
> В **Device Control 1.1.0 и более новых** - по умолчанию по пути **`/opt`**.
> Обязательно копируйте директории с сохранением прав и владельцев. Для копирования используйте стандартные средства, например утилиту **`rsync`**.

13. Чтобы освободить дисковое пространство, вы можете удалить директорию с образами контейнеров прошлых версий `/var/lib/`**`containerd`**.

Для этого выполните команду:

```
rm -rf /var/lib/containerd
```

14. Установите новую версию Device Control (см. *Установка Device Control*).

> **Важно!**
>
> Если вы обновляете Device Control после Device Monitor, обязательно обновите конфигурационный файл `n.yaml`. Подробнее см. шаг 27 *Установки Device Control*.
>
> Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»
>
> С версии 1.1.0 пути установки по умолчанию изменились. Если ранее вы использовали пути `/mnt`, при установке Device Control 1.3.0 и более новых по умолчанию инсталлятор не обнаружит данные прошлой версии и создаст директории по пути `/opt`. Поэтому переместите данные в `/opt`, используйте стандартные средства, например, утилиту `rsync`, или укажите старые директории при установке новой версии.

15. Если до сброса на сервере были установлены и другие продукты, установите версии продуктов, совместимые с Device Control (см. *Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования*).
16. Если Device Control установлен в распределенном кластере, обновите Платформу и продукты на других серверах кластера до версий, совместимых с Device Control.
17. **Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры.**

    Для этого выполните следующие шаги:

    a. Добавьте в файл `/etc/crictl.yaml` (при необходимости создайте его) строки:

    ```
    runtime-endpoint: unix:///run/containerd/containerd.sock
    image-endpoint: unix:///run/containerd/containerd.sock
    timeout: 5
    pull-image-on-create: false
    disable-pull-on-run: false
    ```

    b. Выполните команды:

        i. Для удаления контейнеров Платформы (где x.x.x.x – установленная версия Платформы):

        ```
        crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x|latest/ && $1 ~ /
        docker.infowatch.ru\/platform-core-release/ && $1 !~ /flannel/) {print $3}')
        ```

        ii. Для удаления контейнеров Device Control (где x.x.x.x – установленная версия Device Control):

```
crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x/ && $1 ~ /
docker.infowatch.ru\/devicecontrol/) {print $3}')
```

Данные команды удаляют контейнеры всех версий кроме указанной. Не удаляйте контейнеры установленной версии Device Control и Платформы!

18. Очистите кеш браузера, в котором работали до обновления продукта. Веб-интерфейс Центра расследований доступен по адресу центральной ноды Платформы.

> **Важно!**
>
> Если Device Control установлен **на офисной ноде Платформы в режиме central**, то в результате сброса прошлой установки у добавленных ролей пользователя будет **сброшен доступ к продуктам**. После завершения обновления перейдите в **Настройки** и заново настройте доступ к продуктам в этих ролях (о ролях см. *InfoWatch Device Control. Руководство администратора,* статью *Роли*).

10 Удаление Device Control

Чтобы удалить Device Control:

1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом при установке Device Control.
2. Выполните команду:

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

3. Дождитесь завершения удаления. Программа удалит компоненты Device Control. Данные Device Control удалены не будут. При необходимости вы можете удалить данные вручную из директорий, указанных при установке.
4. Удалите оставшиеся на сервере внутренние пароли Device Control и связанные данные с помощью команд:

   ```
   kubectl delete daemonsets -l product=devicecontrol -n infowatch
   kubectl delete deployments -l product=devicecontrol -n infowatch
   kubectl delete configmaps -l product=devicecontrol -n infowatch
   kubectl delete secrets -l product=devicecontrol -n infowatch
   ```

Примечание:

В случае распределенной установки, если Device Control установлен на офисной ноде и на ней отсутствуют другие продукты, то после удаления Device Control также рекомендуется удалить компоненты платформы. Для этого после выполнения команды `./setup.py remove`, также выполните команду:

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

Если Device Control установлен на центральной ноде или если на офисной ноде вместе с ним также установлены другие продукты, выполнять команду `./setup.py reset` категорически не рекомендуется.

Чтобы узнать, какие продукты установлены в кластере, вы можете перейти в директорию с инсталлятором и выполнить команду:

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