InfoWatch Data Discovery. Руководство администратора

12/01/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Техническая поддержка пользователей 7

4 Лицензирование 8

4.1 Пробная лицензия 8

4.2 Действия с лицензиями 8

5 Настройки системы 9

5.1 Состояние системы 9

5.2 Интеграции 12

5.2.1 Интеграция с Active Directory 13

Информация о интеграциях 15

5.2.2 Интеграция с InfoWatch Traffic Monitor 16

5.2.3 Редактирование и удаление интеграции 19

5.3 Пользователи 20

5.3.1 Создание нового пользователя 20

5.3.2 Добавление нового пользователя из LDAP 22

5.3.3 Редактирование учетной записи 22

5.3.4 Просмотр профиля пользователя 23

5.3.5 Смена пароля пользователя 23

5.3.6 Активация и деактивация пользователя 24

5.3.7 Удаление пользователя 24

5.4 Роли 25

5.4.1 Создание и настройка роли 25

5.4.2 Просмотр, редактирование и копирование роли пользователя 30

5.4.3 Снятие и удаление роли пользователя 31

5.5 Аудит 32

5.6 Настройки пароля 34

5.6.1 Требования к имени пользователя и учетной записи 35

5.7 Основные настройки 35

5.7.1 Сбор статистических данных 35

5.8 Сервисы для уведомлений 36

6 Зоны и серверы 39

6.1 Управление зонами 39
6.1.1 Создание 39
6.1.2 Переименование 39
6.1.3 Удаление 39
6.1.4 Добавление серверов в зону 40
6.1.5 Экспорт данных в Traffic Monitor 40
6.2 Управление серверами 41
6.2.1 Выбор зоны и удаление из зоны 42
6.2.2 Настройка хранилища 43
7 Системные уведомления 46
8 Настройки автоматического удаления событий Data Discovery в Traffic Monitor 47
9 Ротация лог-файлов 48
9.1 Сервисы задач сканирования 48
9.2 Сервис Discoperator 48
9.3 Сервис TPS Agent 48
9.4 Ротация лог-файлов 48
9.5 Настройка ротации с помощью logrotate и crontab 49
10 Добавление пользовательского сертификата 52

Настоящее руководство содержит сведения по настройке и подготовке к работе InfoWatch Data Discovery (далее Система или Data Discovery) – программного обеспечения, предназначенного для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.

1 Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые будут работать с Системой и заниматься ее администрированием. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и MS Windows.

2 Комплект документов

В документацию входят:

- «InfoWatch Data Discovery. Руководство по установке». Документ содержит описание процесса установки, обновления и удаления Системы.
- «InfoWatch Data Discovery. Руководство администратора». Документ содержит информацию по настройке Системы.
- «InfoWatch Data Discovery. Руководство пользователя». Содержит описание работы с задачами сканирования.

Сопутствующая документация по системе InfoWatch Traffic Monitor (далее Traffic Monitor) включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию системы InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

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.

Часы работы службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

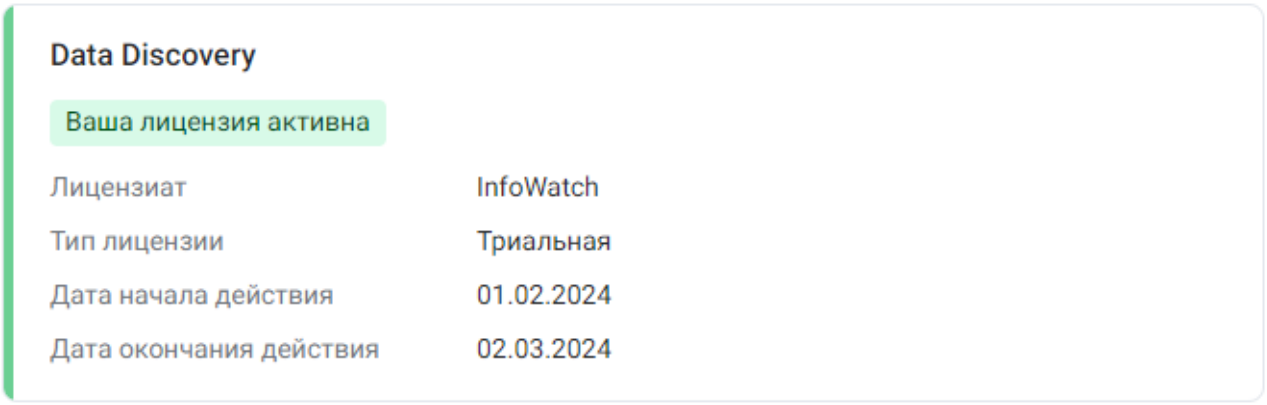
4 Лицензирование

В разделе **Настройки** → **Лицензирование** вы можете управлять лицензиями.

Запуск задач сканирования доступен, только если в Системе есть активная лицензия.

4.1 Пробная лицензия

По умолчанию в Систему добавлена пробная лицензия сроком на один месяц. Дата установки продукта является датой начала действия для этой лицензии.



4.2 Действия с лицензиями

Чтобы добавить лицензию:

1. Нажмите 

;
2. В открывшемся окне добавьте файл лицензии.

Чтобы удалить лицензию:

1. В углу плитки лицензии нажмите ;
2. Выберите **Удалить**;
3. Нажмите **Ок**.

5 Настройки системы

В разделе **Настройки** → **Настройки Системы** содержится информация по следующим настройкам:

- **Состояние системы**
- **Интеграции**
- **Пользователи**
- **Роли**
- **Аудит**
- **Настройки пароля**
- **Основные настройки**
- **Сервисы для уведомлений**

> **Примечание:**
>
> Data Discovery не использует разделы:
>
> - **Данные для анализа** - Data Discovery не хранит данные в партициях и не использует их;
> - **Почтовые уведомления** - Data Discovery не отправляет почтовые уведомления;
> - **Фильтры** - Data Discovery использует отдельные фильтры, которые не переносятся в разделы других продуктов.

5.1 Состояние системы

Подсистема мониторинга выполняет проверку работы всех элементов Системы. При этом анализируется доступность элементов распределенной сети, информация об основных аппаратных компонентах, а также информация о состоянии всех служб Системы.

Раздел **Настройки** → **Состояние системы** содержит панели с информацией о серверах кластера Центра расследований. Каждая панель содержит следующую информацию:

Поле	Описание
Лейбл (имя)	Лейбл и имя ноды в формате `лейбл(имя)`
Статус	Статус ноды: - *Ready* – доступна и готова к работе; - *Not Ready* – не готова к работе; - *Unknown* – зарегистрирована, но не отвечает на запросы.
Адрес	IP-адрес ноды Data Discovery
Последнее обновление состояния системы	Дата и время получения информации о статусе ноды

Поле	Описание
Версия ядра	Версия ядра ОС
Операционная система	ОС ноды Data Discovery
Память	Общий и занимаемый размер оперативной памяти сервера
ЦП	Загрузка центрального процессора сервера Data Discovery
Дисковое пространство (Clickhouse)	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
Дисковое пространство (PostgreSQL)	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
Дисковое пространство (Root)	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Дисковое пространство (NATS)	Общее выделенное и занятое место на диске для хранения данных NATS
Дисковое пространство (Datastorage)	Общее выделенное и занятое место на диске для хранения бинарных данных
Список служб ноды Data Discovery	
Статус	Один из статусов службы: • *Запущена* – работает; • *Остановлена* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть на узле, но отсутствует; • *Ошибка* – завершена с ошибкой.
Имя	Имя службы в Системе *(контейнеры, поды)*
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

Примечание:

Если на сервере установлены и другие продукты Центра расследований InfoWatch, их службы также будут в списке.

Если Data Discovery выполняет задачи сканирования, в списке будут отображаться и службы, относящиеся к запущенным задачам.

Сервисы задач сканирования имеют ряд особенностей:

- В именах сервисов указан номер задачи сканирования, к которым они относятся.
  Например, для задачи с номером 42: `puller-42`, `sender-42`.
- Несколько сервисов одного типа, относящихся к одной задаче, в списке будут отображены с одинаковыми именами;
  Например: если для выполнения задачи сканирования с номером 42 Data Discovery запускает три сервиса puller, в списке будут отображены три записи `puller-42`.
- Сервис, который не запустился или перестал работать, не будет отображаться в списке.

Примечание:

* Если в одном из разделов осталось 10 ГБ или меньше свободного пространства, в веб-интерфейсе Центра расследований будет выведено неотключаемое предупреждение том, что превышено ограничение по использованию дискового пространства.
Если ограничение превышено:

- на **офисной ноде Платформы** - будут остановлены интеграции, настроенные на этой ноде;
- на **центральной ноде Платформы** - будут остановлены все интеграции в кластере.

Чтобы снять это ограничение, в **Настройки** → **Состояние системы** определите ноду и раздел, в котором осталось мало пространства, и освободите его средствами ОС или продукта.
В Data Discovery вы можете настроить лимит для хранилища просканированных файлов (директория по умолчанию: `/opt/disctps`). Подробнее см. "Зоны и серверы".
Если в хранилище осталось мало свободного пространства, вы можете ускорить отправку файлов в Traffic Monitor, для этого в настройках задач сканирования сократите количество сканеров (`puller`) и увеличьте количество передатчиков (`sender`).

Все события мониторинга в Системе записываются в журнал.

Чтобы экспортировать диагностические данные:

1. Нажмите **Экспорт диагностических данных**. В диагностические данные будут добавлены лог-файлы работающих служб и лог-файлы выполняющихся задач сканирования со всех нод Data Discovery. После формирования диагностических данных начнется загрузка.

> **Примечание:**
>
> Для получения лог-файлов задачи сканирования (например, лог-файлов экземпляров сервиса Puller) убедитесь перед экспортом диагностических данных, что задача запущена.

2. Скачайте zip-архив, содержащий txt-файлы с логами.

Чтобы скачать диагностические данные отдельной службы:

1. Нажмите  напротив нужной службы. Начнется формирование лог-файла, а затем загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами службы.

5.2 Интеграции

В разделе **Настройки**  → **Интеграции** вы можете настроить интеграции с источником данных:

- Active Directory – для получения актуального дерева каталогов Active Directory компании и формирования досье;
- InfoWatch Traffic Monitor – для загрузки в Платформу:
  - конфигурации (объекты защиты) Traffic Monitor, которую Data Discovery использует для контентного анализа - обнаружения объектов защиты в извлеченных текстовых контентах;
  - событий Traffic Monitor, которые можно добавлять в расследования, а также для получения данных, используемые другими продуктами.

Интеграция с Active Directory позволяет:

- **Добавлять новых пользователей в Систему из LDAP-каталогов**.
  Пользователи, добавленные из LDAP-каталогов, входят в Систему с помощью доменных учетных данных. Подробнее о добавлении пользователя из LDAP-каталога см. "Добавление нового пользователя из LDAP".
  Для добавления нового пользователя из LDAP-каталога не требуется синхронизация.

- **Добавлять хосты из каталога в задачу сканирования** (см. " InfoWatch Data Discovery. Руководство пользователя", "Добавление и настройка хостов").

- **Добавлять в Систему персон и группы из LDAP-каталогов:**
  - В раздел **Досье** будет выгружен список персон с возможностью просмотреть информацию по каждой;
  - Персоны, добавленные из LDAP-каталогов будут иметь тип контакта SID;
  - Система сможет идентифицировать персон и группы по SID. Их имена будут отображаться в таблице с информацией о файлах (см. " InfoWatch Data Discovery. Руководство пользователя", "Таблица с информацией о файлах").

Для добавления данных в Систему требуется провести синхронизацию.

Подробнее о настройке интеграций см. статьи:

- "Интеграция с Active Directory";
- "Интеграция с InfoWatch Traffic Monitor";
- "Редактирование и удаление интеграции".

Важно!

События, полученные в результате интеграции с InfoWatch Traffic Monitor, не используются для функциональности Data Discovery.

Для настройки экспорта данных в Traffic Monitor см. "Зоны и серверы".

5.2.1 Интеграция с Active Directory

Чтобы добавить интеграцию с Active Directory:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Интеграции**.
2. Нажмите + Добавить.
3. Выберите **Active Directory**.
4. Укажите значения параметров:

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли
Филиал	Лейбл ноды Data Discovery для подключения к Active Directory
Адрес источника	Сетевой адрес сервера Active Directory
Тип соединения	Выбор типа соединения, которое будет установлено: • Незащищенное соединение (Plain) • Защищенное соединение по протоколу LDAP (StartTLS) • Защищенное соединение по протоколу LDAPS (TLS) **Важно:** Соединение без сертификатов небезопасно.
Сертификат	Загрузка файла сертификата в формате PEM или DER Параметр используется, если выбран защищенный тип соединения
Глобальный порт	Порт для подключения глобального LDAP-каталога. По умолчанию используются значения: • 3268 для: • незащищенного соединения (Plain); • защищенного соединения по протоколу LDAP (StartTLS);

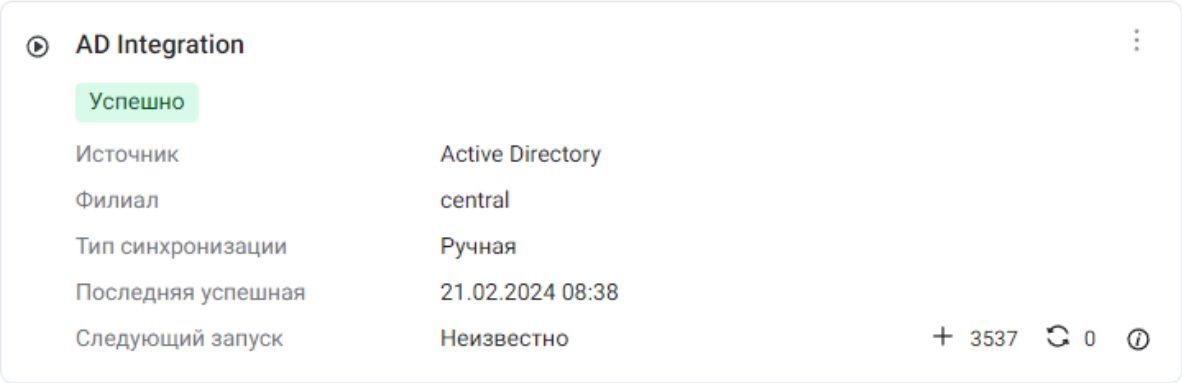
Параметр	Описание
	• 3269 для защищенного соединения по протоколу LDAPS (TLS). Чтобы указать значения, используемые по умолчанию, нажмите 
Порт	Порт для подключения локального каталога домена. По умолчанию используются значения: • 389 для: • незащищенного соединения (Plain); • защищенного соединения по протоколу LDAP (StartTLS); • 636 для защищенного соединения по протоколу LDAPS (TLS). Чтобы указать значения, используемые по умолчанию, нажмите 

LDAP-запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. Может быть указан только один каталог в организационной структуре Active Directory. Для оптимизации поиска вы можете использовать отдельные уровни иерархии базы:
	`C – countryName`
	`O – organizationName`
	`OU – organizationalUnit`
	`DC – domainComponent`
	`CN – commonName`
	Пример: Чтобы использовать в качестве базы поиска ветку Users, расположенную в домене компании, необходимо ввести: `cn=users,dc=company,dc=com`

Логин	Логин для доступа к серверу Active Directory (пользователь должен иметь права на чтение каталога)
Пароль	Пароль для доступа к серверу Active Directory
Синхронизация	Тип синхронизации: ручная или автоматическая. Если выбрана автоматическая синхронизация, то необходимо указать значения в параметрах **Периодичность** и **Повторение**
Периодичность	Интервал проведения автоматической синхронизации. Например, если у параметра **Периодичность** значение **Ежечасно** и у параметра **Повторение** значение **2**, то синхронизация запускается с интервалом в 2 часа.
Повторение	

5. Нажмите **Проверить соединение**, чтобы проверить, что все параметры заполнены корректно, и дождитесь сообщения **Соединение успешно установлено**. В случае появления статуса:
    - **Не удалось установить соединение** – проверьте, что были введены корректные адрес и порт;
    - **Заданы неверные логин или пароль** – проверьте, что были введены корректные логин и пароль.
6. Нажмите:
    - **Сохранить** – чтобы сохранить интеграцию без проведения синхронизации;
    - **Сохранить и синхронизировать** – чтобы сохранить интеграцию и запустить процесс синхронизации немедленно.

> **Важно!**
>
> Синхронизация с Active Directory может создавать высокую нагрузку на сервера домена и сеть, поэтому рекомендуем проводить первую синхронизацию с Active Directory в ночное время.



Чтобы запустить синхронизацию вручную, нажмите  на панели интеграции. Процесс может занять длительное время.

Информация о интеграциях

Синхронизация возможна с несколькими LDAP-каталогами. Каждая интеграция отображается в отдельной панели.

В нижней строке панели указано:

-  – количество добавленных в ходе синхронизаций персон, групп и рабочих станций;
-  – количество персон, групп и рабочих станций, данные которых обновились в ходе последней синхронизации.
-  - детальная информация показывает, сколько персон было добавлено или обновлено в ходе последней синхронизации.

Для каждой интеграции указывается статус синхронизации:

Статус	Описание
НЕ СИНХРОНИЗИРОВАЛОСЬ	Интеграция сохранена, синхронизация еще не разу не запускалась
СИНХРОНИЗИРУЕТСЯ	Идет процесс синхронизации
УСПЕШНО	Синхронизация завершилась успешно
ПРЕРВАНА	Синхронизация остановлена пользователем. В статусе также указаны дата и время остановки
ОШИБКА	Данный статус может обозначать следующее: • введены некорректные логин, пароль, или адрес; • в ходе синхронизации произошла ошибка.

5.2.2 Интеграция с InfoWatch Traffic Monitor

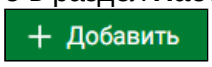
Интеграция с InfoWatch Traffic Monitor используется для загрузки в Центр расследований событий, объектов защиты, а также групп и персон. Добавление персон позволяет заводить досье и инициировать расследования (см. документ "InfoWatch Data Discovery. Руководство пользователя" статью "Создание, редактирование и удаление досье").

Data Discovery использует объекты защиты из Traffic Monitor для контентного анализа - обнаружения объектов защиты в извлеченных текстовых контентах.

> **Примечание:**
>
> Для загрузки объектов защиты в Центр расследований рекомендуется использовать тот же сервер базы данных Traffic Monitor, который был указан при установке Модуля контентного анализа. Это обеспечит согласованность конфигураций в модуле и в Data Discovery. Если в Центре расследований будут отсутствовать данные об объектах защиты, добавленных в модуль, Data Discovery не сохранит по ним результаты контентного анализа.
>
> Data Discovery не использует данные по событиям Traffic Monitor. Функциональность могут использовать другие продукты, установленные в кластере Центра расследований.
>
> Если в кластере нет продуктов, использующих события Traffic Monitor, вы можете не хранить их в Платформе после настройки интеграции.

При первом входе в Систему список интеграций пустой.

Чтобы добавить новую синхронизацию с InfoWatch Traffic Monitor и запустить ее:

1. Перейдите в раздел **Настройки**  → **Настройки системы** → **Интеграции**.
2. Нажмите .
3. Выберите **Infowatch Traffic Monitor** и введите параметры:

Параметр	Описание
Имя интеграции	Название интеграции
Филиал	Нода для подключения: головное отделение или филиал
Адрес источника	Сетевой адрес функционирующего сервера Traffic Monitor
Токен	Ключ, необходимый для получения данных от сервера Traffic Monitor (см. документ "*InfoWatch Data Discovery. Руководство по установке*" статью "*Установка лицензии и плагина Traffic Monitor*")
Количество потоков загрузки	Количество рабочих потоков, через которые загружаются события и справочники из Traffic Monitor. Чем больше потоков, тем выше нагрузка на базу данных Traffic Monitor. Рекомендуется не задавать количество потоков больше, чем количество ядер процессора на сервере Traffic Monitor
Интервал загрузки событий (мин.)	Отрезок времени совершения событий в Traffic Monitor, данные о которых будут загружаться в Систему одним потоком. По умолчанию: 120 минут. Уменьшение данного параметра позволяет снизить нагрузку в TM при отправке данных
Использовать параметры архивирования при загрузке	При включении этого параметра будут загружены события до текущей даты за последние N недель, установленных в настройках архивирования. По умолчанию: 12 недель. Если не включать параметр, то будут загружены события за все время
Не загружать данные LDAP	Включите параметр, если вы хотите загружать из Traffic Monitor только данные для анализа. Включение параметра исключит загрузку в Центр расследований персон, групп и рабочих станций из Traffic Monitor. Если данные уже были добавлены в Центр расследований, включение параметра не удалит их
Загружать детализацию по событиям	При включении этого параметра будет загружена детализация дополнительно к основным получаемым данным в событиях из Traffic Monitor. Параметр позволяет включить отложенную загрузку
Отложенная загрузка	При включении этого параметра загрузка детализированных данных производится в указанное ниже время

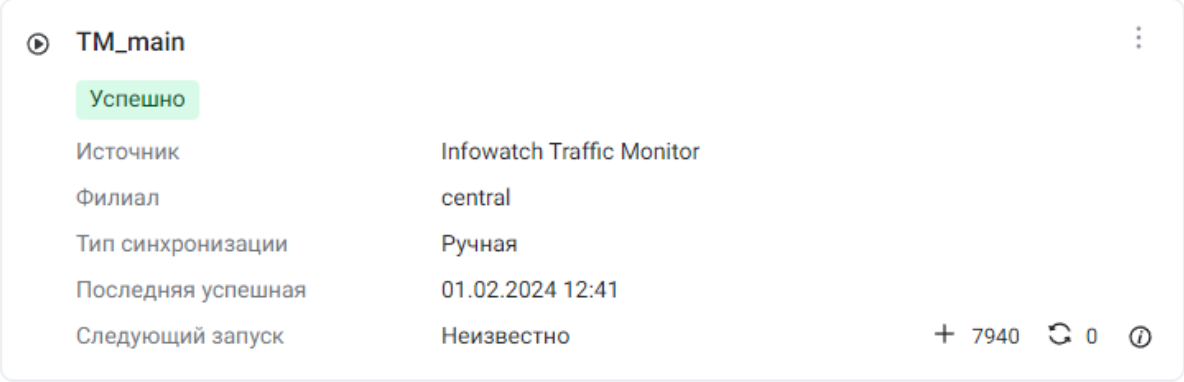
Параметр	Описание
Время отложенной загрузки	Время начала загрузки детализированных данных
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*
Периодичность	Как часто необходимо запускать синхронизацию : *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и/или время следующей синхронизации

4. Нажмите **Проверить соединение**, чтобы проверить полноту и корректность введенных параметров, и дождитесь сообщения "*Соединение успешно установлено*".
5. Нажмите:
   - **Сохранить** – при этом новая синхронизация будет ожидать запуска позднее в статусе *Не синхронизировалось*
   или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации.

Список интеграций с серверами Traffic Monitor отображается в центральной области.

В нижней строке панели указано:

- – количество добавленных сущностей при последней синхронизации;
- – количество сущностей, данные которых обновились в ходе последней синхронизации;
- – детальная информация о результатах синхронизации.



Если необходимо настроить автоматическую синхронизацию по расписанию (например, в ночное время для экономии времени и минимизации нагрузки на сеть):

1. Нажмите и выберите **Редактировать**.
2. Выберите тип синхронизации: **Автоматическая**.
3. Выберите периодичность: **Ежедневно**.
4. Установите время начала: **0:00**.
5. Нажмите **Сохранить**. Система запустит синхронизацию по расписанию.

Важно!

При планировании первичной синхронизации с InfoWatch Traffic Monitor стоит учитывать, что загрузка большого количества событий из БД может сильно уменьшить пропускную способность сети и общее быстродействие сервера и веб-консоли ТМ. Поэтому рекомендуется работы по синхронизации проводить в компании в нерабочее (ночное) время.

Если необходимо провести еще одну синхронизацию с теми же параметрами:

1. Нажмите .
2. Дождитесь выполнения синхронизации. Процесс может занять продолжительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).
3. После успешной синхронизации с Traffic Monitor перейдите в раздел **События** и убедитесь, что данные получены и отображаются в таблице.

Для каждой интеграции указывается статус синхронизации:

Статус	Описание
НЕ СИНХРОНИЗИРОВАЛОСЬ	Интеграция сохранена, синхронизация еще не разу не запускалась
СИНХРОНИЗИРУЕТСЯ	Идет процесс синхронизации
УСПЕШНО	Синхронизация завершилась успешно
ПРЕРВАНА	Синхронизация остановлена пользователем. В статусе также указаны дата и время остановки
ОШИБКА	Данный статус может обозначать следующее: • введены некорректные логин, пароль, или адрес; • отсутствует плагин/лицензия на использование продукта в Traffic Monitor; • в ходе синхронизации произошла ошибка.

5.2.3 Редактирование и удаление интеграции

Чтобы внести изменения в уже созданную интеграцию:

1. Нажмите  в правом верхнем углу и выберите **Редактировать**.
2. Внесите изменения.
3. Нажмите **Сохранить**:
   - Чтобы создать новую интеграцию с указанными настройками вместо текущей интеграции, нажмите **Создать новую**. Текущая интеграция будет удалена.
   - Если требуется изменить настройки интеграции, нажмите **Продолжить в этой**.

Чтобы удалить интеграцию:

1. Нажмите  в правом верхнем углу.
2. Выберите **Удалить**, затем нажмите **Ок**.

> **Примечание:**
>
> Данные, полученные в результате синхронизаций, не будут удалены после удаления интеграции.

5.3 Пользователи

Во время установки Системы создается предустановленный пользователь – Главный офицер. Для входа в Систему введите логин и пароль по умолчанию:

Логин	Пароль
officer	xxXX1234

При первом входе в Систему Офицеру безопасности необходимо сменить пароль на постоянный (см. "Смена пароля пользователя").

Главная страница раздела **Пользователи** содержит список пользователей, допущенных к работе с Системой:

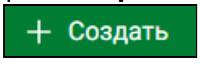
- Главного Офицера безопасности;
- других Офицеров безопасности (ОБ), подчиненных ему.

Действия пользователя:

- Создание нового пользователя
- Добавление нового пользователя из LDAP
- Редактирование учетной записи
- Просмотр профиля пользователя
- Смена пароля пользователя
- Активация и деактивация пользователя
- Удаление пользователя

5.3.1 Создание нового пользователя

Главный офицер может добавить новых пользователей, которые также могут выполнять функции Офицеров безопасности. Для этого:

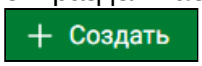
1. Перейдите в раздел **Настройки**  → **Настройки системы** → **Пользователи**.
2. Нажмите справа .
3. Выберите **Создать пользователя**.
4. Введите значения параметров согласно таблице:

Параметр	Обязательный параметр	Описание
Фотография	Нет	Фотография пользователя
Имя пользователя	Да	Имя нового пользователя (о требованиях к имени пользователя см. "Настройки пароля").
Логин	Да	Имя учетной записи пользователя (о требованиях к логину см. "Настройки пароля"). Логин не зависит от верхнего или нижнего регистра
Пароль	Да	Пароль учетной записи (о требованиях к паролю см. "Настройки пароля").
Подтверждение пароля	Да	Пароль учетной записи
Роль	Нет	Роль пользователя в Системе. Пользователю может быть присвоена только одна роль.
Язык консоли	Нет	Язык интерфейса для нового пользователя: *Русский* или *Английский*
Отображать только функции установленных продуктов	Нет	Переключатель, который скрывает для пользователя разделы и виджеты неустановленных продуктов
Контакты	Нет	Email-адрес. Можно добавить одно или несколько значений
	Нет	Номер телефона. Можно добавить одно или несколько значений

5. Нажмите **Создать**. Новый пользователь будет добавлен в Систему. При первом входе в Систему он должен поменять пароль своей учетной записи (см. "Смена пароля пользователя").

5.3.2 Добавление нового пользователя из LDAP

Главный офицер может выбрать из LDAP-каталога новых пользователей, которые также могут выполнять функции Офицеров безопасности. Чтобы добавить нового пользователя в Систему из LDAP-каталога:

1. Перейдите в раздел **Настройки**  -> **Настройки системы** -> **Пользователи**.
2. Нажмите .
3. Выберите **Добавить из LDAP**.
4. Выберите доступный LDAP-сервер, интеграция с которым настроена в Системе (подробнее про интеграцию см. "Интеграция с Active Directory").
5. В строке поиска начните вводить ФИО или логин пользователя.
6. В результатах поиска выберите нужного пользователя и нажмите **Добавить**.
7. Назначьте пользователю роль (см. подробнее "Редактирование учетной записи").

Пользователь будет добавлен в список пользователей Системы. Новый пользователь входит в Систему с помощью доменных учетных данных. Логин учетной записи имеет вид: `domain\login` или `login@domain`. Для логина учетной записи не учитывается регистр.

> **Примечание:**
>
> Требования к безопасности (см. "Настройки пароля") не распространяются на пользователей, добавленных из LDAP-каталога. Для таких пользователей недоступно изменение пароля в Системе.

> **Важно!**
>
> Изменения учетной записи, внесенные в Active Directory, будут доступны в Системе только после повторного добавления учетной записи: учетную запись необходимо удалить, а затем добавить повторно.

5.3.3 Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

1. Перейдите в раздел **Настройки**  -> **Настройки системы** -> **Пользователи**.
2. Нажмите  напротив пользователя или на странице его профиля справа вверху.
3. Выберите **Редактировать**.
4. В открывшемся окне измените одну или несколько настроек. Доступны настройки, заданные при создании пользователя (см. "Создание нового пользователя").
5. Нажмите **Сохранить**. Новые настройки вступят в силу.

Чтобы назначить роль пользователю:

1. Перейдите в раздел **Настройки**  -> **Настройки системы** -> **Пользователи**.
2. Выберите пользователя.
3. В личной карточке пользователя перейдите на вкладку **Права доступа** и нажмите на ссылку Назначить роль.

4. В открывшемся окне в поле **Роль** выберите роль для назначения пользователю в раскрывающемся списке. Пользователь без роли не сможет работать в Системе.
5. Нажмите **Сохранить**.
6. Чтобы применить изменения, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте **Завершить активные сессии пользователей**.
7. Подтвердите действие, нажав **Применить**. Пользователю будет назначена новая роль.

5.3.4 Просмотр профиля пользователя

На странице профиля представлена личная карточка пользователя со следующими данными:

1. Вкладка **Персональная информация** содержит:
   - фото пользователя;
   - имя пользователя;
   - логин пользователя в Системе;
   - язык, используемый пользователем в Системе;
   - контактные данные: номера телефонов, адреса электронной почты;
   - журнал последних активностей с учетной записью.
2. Вкладка **Права доступа** содержит информацию о правах пользователя в Системе:
   - роль, назначенная пользователю;
   - доступные для выполнения функции:
     - доступ, который имеет данный пользователь к настройкам и продуктам;
     - совокупность данных, к которым пользователь имеет доступ.

   Удаление или назначение новой роли осуществляется в окне редактирования учетной записи (см. "Редактирование учетной записи").

Действия пользователя:

- Редактирование учетной записи
- Смена пароля пользователя
- Активация и деактивация пользователя

5.3.5 Смена пароля пользователя

Чтобы сменить выданный пароль при первом входе в Систему или скомпрометированный пароль:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив пользователя;
   - откройте профиль пользователя и нажмите в правом верхнем углу.
3. Выберите **Сменить пароль**.
4. Заполните поля:

Поле	Описание
Старый пароль	Введите действующий пароль

Поле	Описание
Новый пароль	Введите новый пароль. Новый пароль должен удовлетворять настройкам безопасности (см. "Настройки пароля")
Подтверждение пароля	Введите повторно новый пароль

5. Нажмите **Сохранить**.

5.3.6 Активация и деактивация пользователя

Главный офицер может запретить выбранному пользователю выполнять любые действия в Системе. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив активного пользователя;
   - откройте профиль активного пользователя и нажмите в правом верхнем углу.
3. Выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив заблокированного пользователя;
   - откройте профиль заблокированного пользователя и нажмите в правом верхнем углу.
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

Другие офицеры безопасности могут деактивировать пользователей, если у них есть доступ к настройкам пользователей.

5.3.7 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив пользователя;
   - откройте профиль пользователя и нажмите в правом верхнем углу.
3. Выберите **Удалить**.
4. В открывшемся окне нажмите **Ок**. Учетная запись пользователя со всеми данными будет удалена без возможности восстановления.

Примечание:

Учетная запись Главного офицера не может быть удалена.

5.4 Роли

Пользователи Системы могут иметь разные роли, которые определяют их права в Системе. Если пользователю не назначена роль, он не имеет доступа в Систему.

Пользователь, который работает в Системе, имеет только одну **Роль.** Эта **Роль** содержит в себе **Функции** и **Данные**, доступ к которым может быть ***открыт полностью***, ***только на просмотр*** или ***запрещен***

На главной странице раздела **Настройки**  → **Настройки системы** → **Роли** отображены все используемые в Системе роли. Они включают в себя вновь созданные пользовательские роли и две предустановленные:

1. **Главный офицер** – имеет полный доступ ко всем данным Системы, ее настройкам и управлению ролями, включая:
    - создание новых пользователей;
    - создание новых ролей и назначение их пользователям.
2. **Офицер безопасности** – имеет полный доступ к данным Системы, за исключением раздела **Настройки**.

Информация о роли содержится на следующих вкладках:

- **Функции** – доступ пользователя с этой ролью к продуктам, отдельным их функциям и настройкам;
- **Данные** – доступ пользователя с этой ролью к данным;
- **Пользователи** – на вкладке Главный офицер может назначить или снять роль с пользователей.

Роль может быть назначена:

- при создании нового пользователя;
- при создании новой роли;
- добавлена из списка существующих ролей в карточке пользователя на вкладке **Права доступа**.

Действия пользователя:

- Создание и настройка роли
- Просмотр, редактирование и копирование роли пользователя
- Снятие и удаление роли

5.4.1 Создание и настройка роли

Пользователь с ролью **Главный офицер безопасности** может создавать роли и назначать их пользователям. Роль определяет функции пользователя в Системе. Если компетенции пользователя изменились, нужно либо отредактировать роль, либо создать новую роль и назначить ее пользователю. Если у всех пользователей разные компетенции, то необходимо создать столько ролей, сколько пользователей есть в Системе.

Чтобы создать роль:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Роли**.
2. Нажмите **+ Создать**.
3. В открывшемся окне введите название роли и, если необходимо, краткое описание.
4. Нажмите **Сохранить**.
5. На вкладке **Функции** определите доступ пользователя с данной ролью к продуктам и настройкам:
    a. Отметьте в списке **Функции**, к каким из установленных продуктов и к каким их разделам нужно предоставить полный доступ пользователю. По умолчанию пользователь с ролью, не содержащей открытых доступов, сможет авторизоваться в Системе и использовать функционал разделов **Главная** и **Персоны**.

> **Доступ к функциям Центра расследований**
>
> Доступ к *Событиям, Статистике нарушений* дает возможность использовать функционал разделов **События**, **Отчеты**, **Аналитика**, включая виджеты Дата, Отправители, Получатели, Типы событий.
>
> Доступ к *Расследованиям* дает возможность работать в этом разделе.
>
> Доступ к *Деталям событий* дает возможность переходить в Traffic Monitor для получения дополнительной информации о событии, а также использовать:
>
> - виджеты Типы файлов, Топ файлов, Краткий список событий
> - фильтры Имя файла, Наличие вложения, Тип файла, Тема письма
>
> Доступ к *Деталям нарушений* дает возможность выгружать данные о деталях в отчет, использовать:
>
> - виджеты Нарушения, Уровень нарушений, Вердикт, Статистика, Решения пользователя, включая соответствующие им фильтры
> - маркировку событий и раскраску виджетов по уровню нарушений
>
> Доступ к *Политикам, ОЗ, Периметрам* дает возможность использовать:
>
> - виджеты Политики, Объекты защиты, Статистика, включая соответствующие им фильтры
> - дополнительные колонки в разделе **События**
>
> Доступ к *Статусам досье* дает возможность использовать атрибут фильтра и виджет Статусы в досье персоны

> **Доступ к функциям продуктов**
>
> - **Activity Monitor**
>
> Доступ к *Аналитике* дает возможность использовать:
>
> - статистику и события активности в разделах **Аналитика** и **Мониторинг**
> - соответствующие доступным виджетам атрибуты фильтра для событий активности
> - виджеты Activity Monitor в разделе **Персоны** и на **Главной** странице

- функционал отчетов В разделах **Аналитика**, **Мониторинг** и **Отчеты**

Доступ к *Снимкам экрана* дает возможность:

- отображать снимки экрана в разделах **Мониторинг** и **Персоны**
- отображать и фильтровать связанные с ними события

Доступ к *Аудиозаписям* дает возможность:

- отображать данные по аудиозаписям в разделах **Мониторинг** и **Персоны**
- отображать и фильтровать связанные с ними события

Доступ к *Видеозаписям* дает возможность:

- отображать данные по видеозаписям в разделах **Мониторинг** и **Персоны**

Доступ к *Наблюдению* дает возможность функционал наблюдения и таймлайн в разделах **Мониторинг** и **Персоны**

Доступ к *Онлайн* н*аблюдению* дает возможность:

- просмотру экрана персоны,
- прослушиванию звукового окружения персоны,
- блокировке сессии персоны,
- запросить список запущенных процессов на компьютере персоны

Доступ к *Вводимому тексту* дает возможность:

- отображать введенный текст в связанных событиях,
- фильтровать по наличию введенного текста

Доступ к *Поисковым запросам* дает возможность:

- отображать поисковые запросы в связанных событиях
- фильтровать по наличию поисковых запросов

Доступ к *Действиям с файлами* дает возможность:

- отображать действия с файлами и связанные с ними события в разделах **Мониторинг** и **Досье**
- фильтровать события по действиям с файлами
- выгружать отчеты в разделе **Мониторинг**

- **Data Access Tracker**

  Доступ к *Инфраструктуре* дает возможность использовать вкладки в разделе **Инфраструктура**:

  - виджеты продукта Data Access Tracker на вкладке **Сводка** (а также на **Главной** странице в дашбордах);
  - отчеты о состоянии и изменениях объектов службы каталогов на вкладках **Аудит службы каталогов** и **Изменения групп**;
  - отчеты о доступе к почтовым ящикам на вкладке **Права на почтовые ящики**;
  - отчеты об изменениях прав доступа к папкам и файлам на вкладке **Изменения прав на файлы и папки**.

- **Data Discovery**

  Доступ к *Хранению файлов* дает возможность:

  - работать **в разделе Хранение файлов**:

- на вкладке **Задачи** - создавать и запускать задачи сканирования;
- на вкладках **Информация о файлах**, **Дубликаты файлов, Похожие файлы** - анализировать результаты сканирования, контентного анализа и группировки файлов по дубликатам или похожим.

- работать **в досье персон на вкладке Хранение файлов**, которая включает в себя подразделы:
  - **Владелец файлов**
  - **Доступные файлы**
- выгружать отчеты с информацией из подразделов **Владелец файлов** и **Доступные файлы** досье персоны, а также - из вкладок **Информация о файлах**, **Дубликаты файлов** и **Похожие файлы** раздела **Хранение файлов**

- **Prediction**

  Доступ к *Досье, Рейтинг* дает возможность:

  - работать с рейтингом персон и карточками групп риска в разделе **Риски**
  - работать в досье персоны на вкладках **Группы рисков** и **Карта паттернов**
  - отображать виджеты Prediction на **Главной** странице в дашбордах
  - выгружать отчеты в разделе **Риски** и на вкладке **Группы рисков** в досье персоны

- **Vision**

  Доступ к *Графу связей* дает возможность использовать функционал графа.

  Доступ к Статистике нарушений дает возможность работать со:

  - статистикой в разделах **Аналитика** и **Персоны**, выгружать отчеты
  - виджетами Vision на **Главной** странице
  - файлами отчетов в разделе **Отчеты**

  Доступ к *Комментариям и файлам в Досье* дает возможность:

  - использования виджетов Комментарии и Файлы в досье персоны,
  - сформировать выгрузку или скриншот виджета или графа с сохранением в досье

b. Отметьте в списке **Настройки**:
   -  - если нужен полный доступ (просмотр и редактирование) к настройкам в разделе . По умолчанию доступ запрещен;
   -  - если нужны права только на просмотр ;
   -  - если нужно запретить доступ к отдельным разделам.
     При этом доступ к персональной информации в собственном профиле у пользователя есть всегда.

6. На вкладке **Данные** вы можете настроить доступ к данным для пользователя. Для изменения прав доступа к выборочным данным, укажите их в категориях: Персоны, Группы, Отделы, Контакты, Филиалы, Политики, Объекты защиты. При этом можно:

- ☐ - ограничить доступ к выбранным данным;
- ☑ - разрешить доступ к выбранным данным;
- ☒ - закрыть доступ к выбранным данным.

Пример:

Если отметить Персону знаком ☒, то эта роль запретит пользователю доступ к любой информации о ней в Системе.

Если отметить Персону знаком ☑ (или оставить по умолчанию ☐ у всех Персон), то эта роль предоставит пользователю полный доступ к данным персоны: событиям, досье, в Едином фильтре, отображениях на Графе связей и виджетах.

Если отметить Персону знаком ☐ при одновременном выборе других Персон, то эта роль предоставит пользователю доступ к ее событиям с участием разрешенных участников (☑), но без доступа к любым отображениям на Графе связей, виджетах и в Едином фильтре.

Примечание:

Главному офицеру безопасности необходимо внимательно следить за добавляемыми условиями, так как в случае использования различных элементов в роли может получиться не расширение, а сужение доступных данных из-за использования между разными категориями оператора И.

Например:

a. Был настроен доступ к Группе-1 ИЛИ Группе-2.
b. Добавили доступ к Персоне-1, Персоне-2, Персоне-3.
   В итоге количество доступных пользователю данных уменьшилось, потому что получилось условие:
   (Группа-1 ИЛИ Группа-2) И (Персона-1 ИЛИ Персона-2 ИЛИ Персона-3).

Чтобы настроить общее ограничение и на группы и на персоны, создайте в Traffic Monitor сводную группу, которая включает в себя все необходимые группы и персоны. Используйте ее в настройках доступа.

Правильность добавления новых областей видимости и исключений следует проверять путем задания аналогичных условий в Едином фильтре, и далее проверять результаты на виджетах.

7. Если требуется закрыть доступ ко всем данным, отметьте ☑ **Запретить доступ к данным.**

Примечание:

Для корректной работы с Data Discovery не запрещайте пользователю доступ к данным.

8. На вкладке **Пользователи** выберите доступного пользователя без роли, которому необходимо назначить данную роль. Для этого:
   a. Нажмите **+ Добавить**.

b. В открывшемся диалоговом окне выберите пользователя в поле **Пользователи**.
c. Нажмите **Выдать**. Роль будет назначена данному пользователю.

9. После внесения всех настроек нажмите **Применить**.
10. Для применения настроек, пользователи должны выйти из системы и повторно авторизоваться. До выхода из системы будут распространяться старые правила ролевого доступа. Чтобы принудительно завершить сессии пользователей с данной ролью, отметьте **Завершить активные сессии пользователей** в открывшемся окне, а затем **Применить.**

5.4.2 Просмотр, редактирование и копирование роли пользователя

Главный офицер может просматривать и редактировать выданные пользователям роли в их личных профилях. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Роли**.
2. Выберите пользователя, профиль которого необходимо просмотреть. На странице профиля представлена карточка пользователя с его личными данными.
3. Перейдите на вкладку **Права доступа**. На вкладке содержится информация о назначенной пользователю роли, а также:
   - функции– имеет ли пользователь доступ к настройкам продукта;
   - данные (области видимости) – совокупность данных, к которым пользователь имеет доступ.
4. Чтобы поменять роль пользователю, нажмите и выберите **Редактировать**.
5. В открывшемся окне сначала удалите настоящую роль, нажав .
6. Назначьте новую роль, нажав и выбрав необходимую роль из списка.
7. Нажмите **Сохранить**.
8. Для применения настроек пользователь должен выйти из Системы и повторно авторизоваться. Чтобы принудительно завершить сессию пользователей с данной ролью, отметьте **Завершить активную сессию пользователя** в открывшемся окне, а затем нажмите **Применить**.

Чтобы скопировать любую роль пользователя, например, при расширении штата или для аудиторской проверки:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Роли**.
2. Нажмите на плашке роли, которую необходимо скопировать и выберите **Копировать роль**. При этом будут скопированы следующие атрибуты роли:
   - **Название** – при каждом копировании роли к названию будет добавляться слово **Копия**, пока не получится уникальное название роли:

   Пример: Название *Офицер* в результате копирования поменяется на *Офицер копия*. Чтобы переименовать роль, отредактируйте ее;

   - **Описание**;
   - **Настройки доступа** – копируются все настройки: элементы функций и данных;
   - **Дата создания** – указываются текущие дата и время.

Список пользователей, которым выдана роль, не копируется.

5.4.3 Снятие и удаление роли пользователя

Пользователь не может иметь несколько ролей одновременно. Поэтому если требуется выдать пользователю новую роль, нужно снять действующую.

Чтобы снять роль в карточке роли:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Роли**.
2. Выберите роль, которую необходимо удалить для пользователей.
3. Перейдите на вкладку **Пользователи**.
4. Отметьте пользователей, у которых необходимо снять данную роль.
5. Нажмите **Удалить**. Для данных пользователей роль будет снята. После этого можно назначить им другую роль.
6. Нажмите **Применить**.

Чтобы снять роль в карточке пользователя:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Пользователи**.
2. Выполните одно из следующих действий:
   - Нажмите на плашке пользователя, для которого необходимо удалить данную роль.
   - Выберите пользователя и затем нажмите в его личной карточке.
3. В меню выберите **Редактировать**.
4. В открывшемся окне в поле **Роли** удалите роль пользователя, нажав .
5. Нажмите **Сохранить**.
6. Чтобы применить изменения, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте **Завершить активную сессию пользователя**.
7. Подтвердите действие, нажав **Применить**. У данного пользователя роль будет снята.

Главный офицер может удалять любые роли, кроме предустановленных.

Чтобы удалить роль из Системы:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Роли**.
2. Выполните одно из следующих действий:
   - Нажмите на плашке пользовательской роли, которую требуется удалить.
   - Выберите роль и затем нажмите .
3. В окне меню выберите **Удалить**.
4. Чтобы применить изменения, пользователи с данной ролью должны выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессий данных пользователей, в открывшемся диалоговом окне отметьте **Завершить активные сессии пользователей**.
5. Подтвердите действие, нажав **Удалить**. Если роль была назначена пользователям, она будет снята для них и удалена из списка ролей.

5.5 Аудит

В разделе отображается журнал действий пользователей в Системе. Данные журнала может просматривать только пользователь, которому разрешен доступ к разделу (подробнее см. "Роли").

Журнал содержит следующую информацию:

- **Пользователь** – пользователь, который совершил действие;
- **Действие в системе** – действие, которое было выполнено над объектом;
- **Тип объекта**: пользователь, интеграция, досье, роль;
- **Объект события** – название объекта, над которым было совершено действие (например, название роли или интеграции);
- **Филиал** – название филиала, где было зафиксировано событие аудита;
- **Дата** – дата и время создания события аудита.

> **Примечание:**
>
> События в журнале аудита хранятся бессрочно и удалению не подлежат.

Выполняется аудит следующих действий:

Пользователи	- вход в систему - выход из системы - создание - изменение - удаление - изменение пароля - блокировка пользователя
Роли	- создание - изменение - удаление
Интеграции	- создание - изменение - удаление - ручной запуск
Досье	- просмотр - создание - изменение - удаление - объединение

В разделе Аудит вы можете:

- Переместить колонки в таблице (при выгрузке отчета сохраняется порядок по умолчанию);
- Отсортировать содержимое колонок (по умолчанию события отсортированы от последних к наиболее ранним);
- При нажатии на пользователя – перейти в его карточку в разделе Пользователи;
- Добавить и удалить фильтры на панели;
- Отсортировать события, выбрав фильтры;
- Выгрузить отчет с событиями аудита (в формате .csv);
- Скопировать содержимое ячейки в таблице.

По умолчанию в разделе отображаются все фильтры:

- *Дата события*;
- *Действие в системе*;
- *Объект события*;
- *Пользователь*;
- *Тип объекта*;
- *Филиал*.

Для управления фильтрами воспользуйтесь кнопкой . Установите флаг , чтобы добавить фильтр на панель, или снимите флаг, чтобы удалить фильтр из набора.

Вы можете отсортировать события:

- выбрав атрибут фильтра на панели над таблицей;
- выбрав нужный атрибут фильтр непосредственно в таблице.

Для этого:

1. Наведите курсор на содержимое ячейки.
2. Во всплывающем окне нажмите **Добавить в фильтр** . Содержимое таблицы будет отсортировано в соответствии с выбранным атрибутом.

Чтобы скопировать содержимое ячейки:

1. Наведите курсор на содержимое ячейки.
2. Во всплывающем окне поместите курсор на строку с содержимым, затем нажмите **Копировать** .

В колонке **Дата** кнопка **Копировать** отображается справа при наведении курсора на содержимое ячейки.

Чтобы выгрузить отчет с выбранными событиями аудита:

1. Нажмите **Сохранить отчет** .
2. Перейдите в папку **Загрузки** вашего компьютера.

При выгрузке сохраняется порядок колонок в таблице по умолчанию.

Для просмотра отчета в Excel необходимо поменять кодировку на utf-8. Подробнее об этом см. статью в базе знаний "Как сменить кодировку файла на UTF-8 в Excel".

5.6 Настройки пароля

Чтобы предотвратить несанкционированный вход в Систему и максимально обезопасить пользователя от компрометации его учетных данных третьими лицами, Офицер безопасности может устанавливать правила формирования паролей учетных записей и их сроки действия. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Настройки пароля**.
2. В открывшемся окне установлены настройки по умолчанию. Чтобы ввести новые требования к паролю учетной записи, измените значения параметров:

Параметр	Описание
Буквы	Заглавные и строчные буквы русского и латинского алфавитов, которые используются для составления пароля. Можно установить: - обязательно для ввода ( ) – обязательно присутствие букв в пароле - опционально ( ) – допускается пароль без букв
Цифры	Арабские цифры, которые используются для составления пароля. Можно установить: - обязательно для ввода ( ) – обязательно присутствие цифр в пароле - опционально ( ) – допускается пароль без цифр
Специальные символы	Перечень спецсимволов, которые могут быть в пароле. Можно установить: - обязательно ( ) – обязательно присутствие спецсимволов в пароле - опционально ( ) – допускается пароль без спецсимволов
Минимальная длина	Минимально допустимая длина пароля в символах
Невозможно использование последних N паролей	Чтобы избежать компрометации, запрещено использовать пароли за предыдущие периоды
Срок действия пароля	Количество дней действия пароля. До истечения указанного срока пароль необходимо сменить
Период неудачных попыток авторизации	Период (в минутах), в течение которого пользователь может вводить неверный пароль

Параметр	Описание
Количество неудачных попыток ввода	Количество неуспешных попыток ввода пароля, после которого учетная запись будет заблокирована
Период блокировки пользователя	Период блокировки учетной записи (в минутах)

3. Нажмите **Сохранить**, чтобы активировать новые значения параметров. Если нужно вернуться к прежним настройкам, нажмите **Сбросить настройки до значений по умолчанию**.

> **Пример**
>
> `Период неудачных попыток авторизации – 5.`
> `Количество неудачных попыток ввода – 4.`
> `Период блокировки пользователя – 15.`
>
> Если установлены указанные значения параметров, то после 4 неудачных попыток ввода пароля в течение 5 минут учетная запись пользователя будет заблокирована на 15 минут. После этого можно будет повторить ввод пароля.

5.6.1 Требования к имени пользователя и учетной записи

Имя пользователя должно содержать не менее четырех символов.

Логин пользователя:

- должен начинаться с буквы и не заканчиваться точкой
- может состоять из букв латинского алфавита, арабских цифр и содержать спецсимволы: "_", "-", "–", "."

5.7 Основные настройки

В разделе **Настройки** → **Основные настройки** вы можете управлять сбором статистических данных.

> **Важно!**
>
> Другие настройки этого раздела не используются для Data Discovery.

5.7.1 Сбор статистических данных

Система сбора статистики накапливает и обобщает данные о работе пользователя в Консоли управления. По решению пользователя эти данные могут быть скачаны и отправлены в компанию

InfoWatch для обработки. Это делается для повышения качества продукта, оценки востребованности той или иной функциональности и разработки новых сценариев работы.

Сбор статистических данных включен по умолчанию. Чтобы отключить сбор данных, снимите флажок в поле **Включить** и нажмите **Сохранить**.

> **Примечание:**
>
> Система сбора статистики не накапливает, не анализирует и не передает персональные данные. Все ФИО пользователей и сотрудников заменяются на внутрисистемные ID-номера.

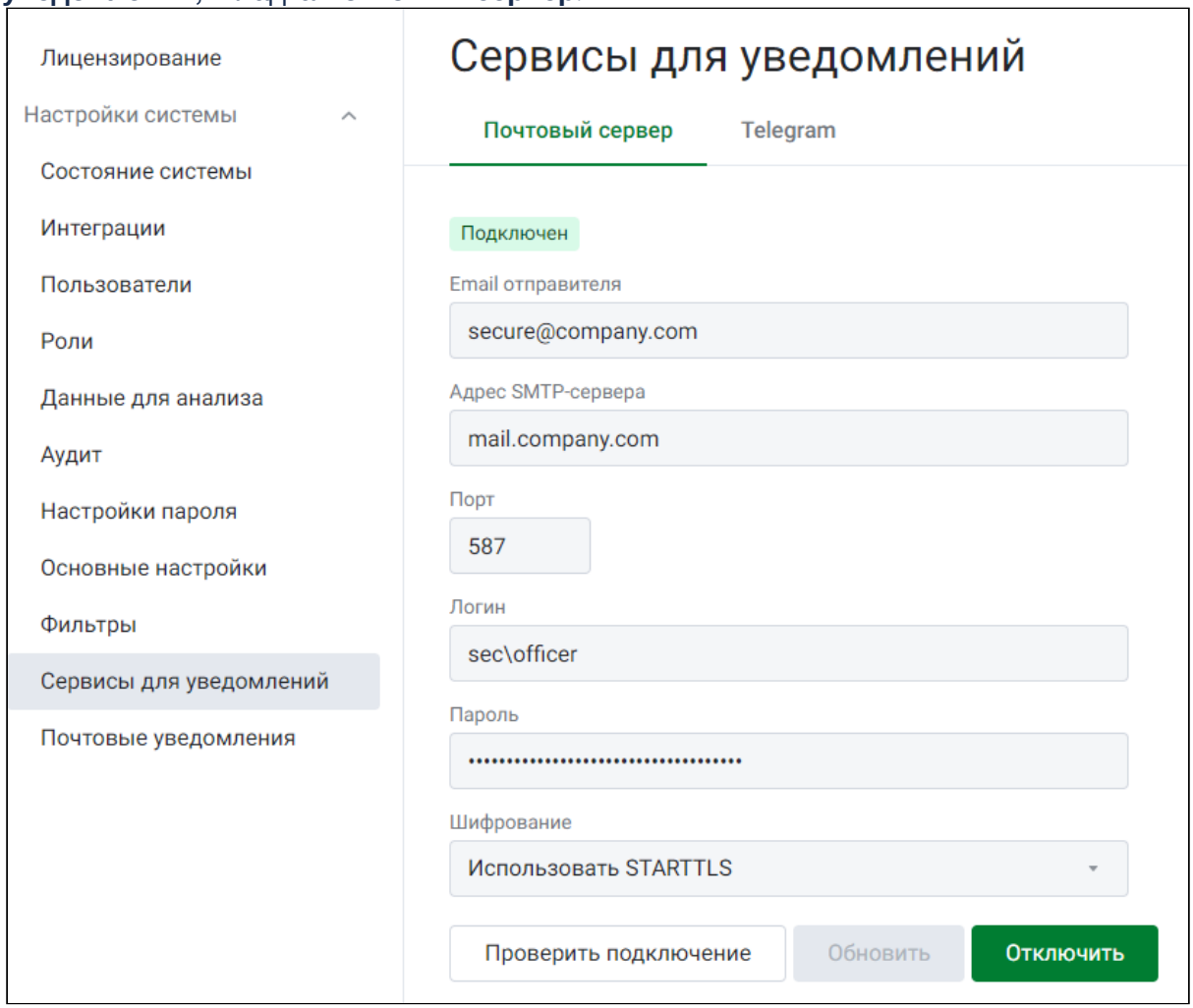
5.8 Сервисы для уведомлений

Для регулярной отправки отчетов Data Discovery использует почтовый сервер.

> **Примечание:**
>
> В текущей версии не поддерживается отправка через Telegram.

Для подключения к почтовому серверу:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Сервисы для уведомлений**, вкладка **Почтовый сервер**.



2. Укажите параметры подключения:

Параметр	Описание
Email отправителя	Адрес электронной почты, от имени которого будут приходить уведомления
Адрес SMTP-сервера	Адрес почтового сервера, работающего по протоколу SMTP. Укажите доменное имя или IP-адрес
Порт	Порт подключения к почтовому серверу
Логин	Имя учетной записи, имеющей доступ к почтовому серверу
Пароль	Пароль учетной записи, имеющей доступ к почтовому серверу

Параметр	Описание
Шифрование	Укажите протокол шифрования, который будет использован при подключении к почтовому серверу. Доступные протоколы: • STARTTLS • TLS

Все поля обязательны для заполнения.

3. После указания параметров подключения нажмите внизу кнопку **Подключить**.
   При успешном подключении Статус изменится на **Подключен**.
   Для проверки доступности сервера внизу есть кнопка **Проверить подключение**.

Чтобы изменить параметры подключения или подключиться к другому почтовому серверу, внесите изменения и нажмите внизу кнопку **Обновить**.

Чтобы разорвать соединение с почтовым сервером, внизу нажмите кнопку **Отключить**.

6 Зоны и серверы

В разделе **Настройки** → **Настройки продуктов** → **Зоны и серверы** вы можете управлять зонами и серверами Data Discovery.

Зона – группа серверов Data Discovery. Разделение серверов на зоны позволяет:

- Запускать сервисы задач только на определенных серверах. В зону могут входить несколько серверов из кластера Системы. Каждый сервер может входить только в одну зону.
- Настраивать экспорт данных в Traffic Monitor для каждой группы серверов. Каждая зона имеет отдельные настройки для экспорта данных.

Вы можете выбрать зону задачи сканирования в настройках задачи (см. *"InfoWatch Data Discovery. Руководство пользователя"*, "*Создание, настройка и запуск задачи*").

6.1 Управление зонами

На вкладке **Зоны**:

- Слева отображается список зон.
- В рабочей области справа отображаются настройки экспорта данных в Traffic Monitor и список серверов зоны.

6.1.1 Создание

Чтобы создать зону:

1. Перейдите на вкладку **Зоны**.
2. Нажмите + Создать зону.
3. Введите имя зоны.
4. Нажмите **Создать**.

6.1.2 **Переименование**

Чтобы переименовать зону:

1. Перейдите на вкладку **Зоны**.
2. Слева отображается список зон. Нажмите справа от имени зоны.
3. Выберите **Переименовать**.
4. Введите новое имя зоны.
5. Нажмите **Сохранить**.

6.1.3 **Удаление**

Если вы удалите зону, сервера будут удалены из зоны. Система на серверах не будет удалена.

Вы не можете удалить зону, если зона выбрана в задачах. Измените зону в настройках задач или удалите такие задачи.

Вы не можете удалить предустановленную зону **По умолчанию**.

Чтобы удалить зону:

1. Перейдите на вкладку  **Зоны**.
2. Слева отображается список зон. Нажмите  справа от имени зоны.
3. Выберите  **Удалить**.
4. Нажмите **Удалить**.

6.1.4 Добавление серверов в зону

Чтобы добавить серверы в зону:

1. Перейдите на вкладку  **Зоны**.
2. Слева отображается список зон. Выберите зону.
3. Нажмите  **Добавить сервер** в рабочей области справа.
4. В открывшемся окне отображаются серверы, которые не добавлены ни в одну зону. Выберите серверы.
5. Нажмите **Добавить**.
6. Перезапустите задачи в зоне, чтобы сервисы задач могли запускаться на добавленных серверах.

6.1.5 Экспорт данных в Traffic Monitor

Чтобы отправлять копии файлов и информацию о файлах в Traffic Monitor для анализа в процессе выполнения задачи сканирования, настройте экспорт данных. Для экспорта данных необходимы плагин и лицензия Traffic Monitor (см. "Установка лицензии и плагина Traffic Monitor").

Чтобы настроить экспорт данных:

1. Перейдите на вкладку  **Зоны**.
2. Слева отображается список зон. Выберите зону
3. Разверните панель **Экспорт данных в Traffic Monitor**.
4. Укажите значения параметров:
   a. **Версия ТМ**:
   Версия Traffic Monitor на сервере, к которому необходимо подключиться. Выберите **Версия 6.10** или **Версия 7.1 и выше**.

   > **Примечание:**
   >
   > Чтобы узнать номер версии ТМ, перейдите в Консоли управления Traffic Monitor в раздел **Офицер безопасности → О системе**.

   b. **Адрес XAPI**:
   Адреса XAPI серверов Traffic Monitor. Серверы должны входить в один кластер Traffic Monitor. Data Discovery отправляет данные на серверы из списка.
   - Чтобы добавить адрес:
     i. Введите адрес в формате IP-адреса IPv4: "xxx.xxx.xxx.xxx".
     ii. Нажмите Enter.

- Вы можете указать несколько адресов.

  > **Примечание:**
  >
  > Чтобы распределять нагрузку и не заполнять файлами только первый указанный сервер Traffic Monitor, Data Discovery использует алгоритм распределения Round-robin: первый файл очереди будет отправлен на первый указанный сервер Traffic Monitor, второй файл будет отправлен на следующий сервер и тд.
  >
  > Распределение нагрузки между несколькими Модулями контентного анализа происходит аналогично.

  Если один адрес недоступен, Система автоматически начинает использовать следующий указанный адрес.
- Traffic Monitor версии 7.7 или выше сообщает, если на сервере недостаточно места для получения данных от Data Discovery (см. "Traffic Monitor. Справочник по конфигурационным файлам", параметры `FreeSpaceThresholdMountPoint` и `FreeSpaceThresholdGb` в **xapi.conf**). В этом случае Data Discovery переключается на следующий адрес XAPI или повторно пытается отправить данные через 1 минуту.

c. **Токен**:
Токен для подключения.

> **Примечание:**
>
> Чтобы скопировать токен для подключения:
>
> i. В Консоли управления Traffic Monitor перейдите в раздел **Управление** -> **Плагины**.
> ii. Выберите в левой верхней части экрана предустановленный плагин:
> - "InfoWatch Crawler" для Traffic Monitor версии 7.3 и ниже;
> - "InfoWatch Data Discovery" для Traffic Monitor версии выше 7.3.
>
> iii. Скопируйте предоставленный токен, нажав .

5. Вы можете проверить доступность серверов Traffic Monitor с помощью кнопки **Проверить соединение**.
6. Нажмите **Применить**.
7. Перезапустите задачи в зоне. Задачи получат новые настройки экспорта данных при запуске.

6.2 Управление серверами

На вкладке **Серверы** отображается список всех серверов Data Discovery. Список серверов для каждой зоны отображается на вкладке **Зоны**.

На панели сервера отображается следующая информация:

Данные сервера	Описание
 Имя	Лейбл и имя сервера в формате: `лейбл(имя)`
 Зона	Зона, в которую добавлен сервер. Значение отсутствует, если сервер не добавлен зону. • Сервер с Data Discovery в режиме central автоматически добавляется в зону **По умолчанию**. • Серверы с Data Discovery в режиме office не добавляются в зоны автоматически.
 Роль	Роли описывают функциональные возможности и назначения серверов, а также дают понять, какие компоненты установлены: • **Сканер и передатчик** - сервер, на котором установлен Data Discovery. Если в зоне нет сервера с этой ролью, запуск задач сканирования в ней невозможен; • **Контентный анализ** - сервер, на котором установлен Модуль контентного анализа. Если в зоне нет сервера с этой ролью, режим **Проводить контентный анализ файлов** в ней недоступен. Если на сервере установлены и Data Discovery, и Модуль контентного анализа, у него будут активны обе роли.
 Хранилище	Данные о пространстве в хранилище сервера

6.2.1 Выбор зоны и удаление из зоны

Примечание:

Вы не можете изменить зону сервера или удалить сервер из зоны, если в хранилище сервера есть файлы задач.

Чтобы получить количество файлов задач в хранилище сервера:

1. Подключитесь к ssh-консоли сервера. Файлы задач хранятся в директориях `PATH/NUMBER`, где:
   - `PATH` – путь к хранилищу сервера, по умолчанию: `/opt/disctps`;
   - `NUMBER` – номер задачи сканирования.
2. Выполните команду `ls PATH/NUMBER -1 | wc -l` для каждой задачи. Пример: `ls /opt/disctps/7 -1 | wc -l`

Чтобы удалить файлы из хранилища, выполните одно из действий для каждой задачи в хранилище:

- Отправьте файлы задачи в Traffic Monitor:

1. В настройках задачи:
    - Включите параметр **Отправлять файлы на анализ в Traffic Monitor**.
    - В настройках задачи укажите следующие значения:
        - **0** для параметра **Число сканеров**;
        - **N** для параметра **Число передатчиков**, где **N** больше или равно количеству серверов Data Discovery в зоне задачи.
2. Запустите задачу. Система отправляет файлы в Traffic Monitor и удаляет их из хранилищ, но не скачивает новые файлы в хранилища зоны.
3. Дождитесь, когда в хранилище не останется файлов задачи.
4. Остановите задачу.

- Удалите задачу. Файлы будут удалены и не будут отправлены в Traffic Monitor.

Чтобы добавить сервер в зону / изменить зону сервера:

1. Нажмите  на панели сервера.
2. Выберите  **Выбрать зону**.
3. Выберите зону в списке.
4. Нажмите **Применить**.
5. Перезапустите задачи в новой зоне сервера, чтобы сервисы задач могли запускаться на этом сервере.

Чтобы удалить сервер из зоны:

1. Нажмите  на панели сервера.
2. Выберите  **Удалить из зоны**.
3. Нажмите **Удалить**. Система на сервере не будет удалена.

6.2.2 Настройка хранилища

Каждый сервер Data Discovery имеет хранилище для просканированных файлов. Все серверы имеют одинаковый путь для хранилища (по умолчанию: `/opt/disctps`). Путь для хранилища указывается при установке Системы на центральном офисе.

Примечание:

Рекомендуется, чтобы хранилище сервера находилось в отдельном разделе или диске.

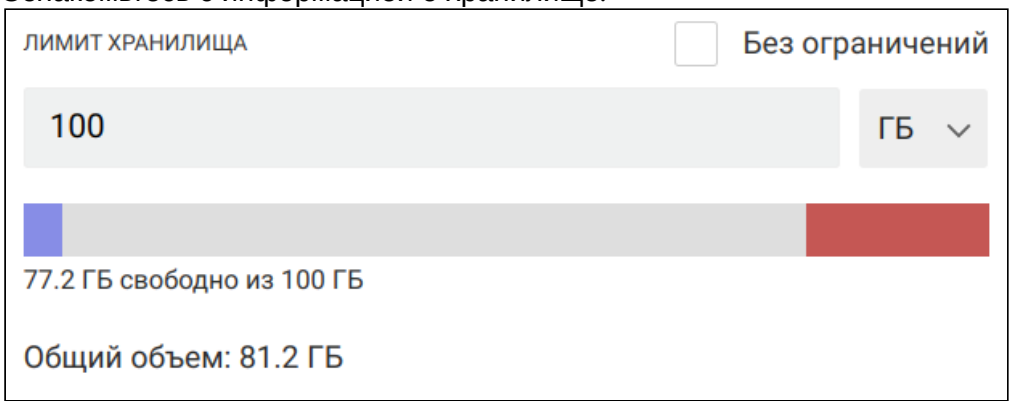
Важно!

В хранилище должны находиться только файлы и директории, которые были добавлены Системой. Если вы добавите другие файлы или директории в хранилище, Система может работать некорректно.

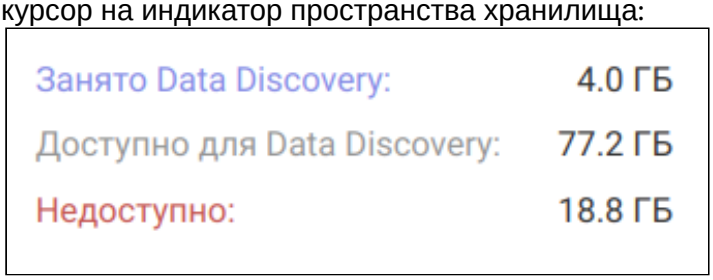
Во время сканирования Система скачивает файл в одно из хранилищ зоны. Файл удаляется из хранилища после отправки в Traffic Monitor.

Чтобы настроить хранилище:

1. Нажмите ⋮ на панели сервера.
2. Выберите ⚙ **Настроить роли.**
3. Ознакомьтесь с информацией о хранилище:



   - В поле **Лимит хранилища** указан текущий лимит.
   - Если включена настройка **Без ограничений**, то лимит хранилища не используется.
   - **Общий объем** = свободное пространство на диске + пространство, которое занято файлами Data Discovery.
4. Чтобы просмотреть подробную информацию о пространстве в хранилище, наведите курсор на индикатор пространства хранилища:



   - **Занято Data Discovery** – пространство, которое занято файлами Data Discovery.
   - **Доступно для Data Discovery** – свободное пространство на диске, которое Data Discovery может использовать.
   - **Недоступно** – отображается, если лимит превышает **Общий объем** хранилища.
5. Настройте лимит:

> **Важно!**
>
> Установите лимит для хранилища, если Система и хранилище расположены в одном разделе. Рекомендуется настроить лимит так, чтобы в разделе всегда было доступно 10 ГБ.
>
> Система может работать некорректно, если в разделе недостаточно свободного места.

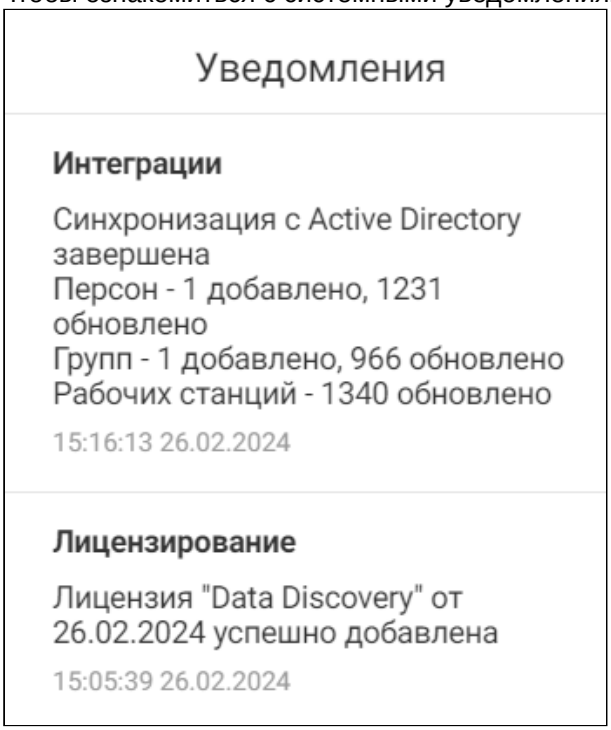
   - Чтобы установить лимит:
     a. Отключите настройку **Без ограничений**.
     b. Укажите лимит в поле **Лимит хранилища** и выберите единицу измерения. Система остановит загрузку файлов в хранилище, если занятое место в хранилище достигнет лимита. Если место освободится, Система продолжит загрузку.

- Если лимит не требуется, включите настройку **Без ограничений**. Система остановит загрузку файлов в хранилище, если закончится свободное место на диске. Если место освободится, Система продолжит загрузку.

6. Нажмите **Применить**. Система начнет использовать новые настройки хранилища.

7 Системные уведомления

Чтобы ознакомиться с системными уведомлениями Центра расследований, нажмите .



Уведомления сообщают о:

- статусе синхронизаций с различными источниками, которые инициировал пользователь;
- добавлении лицензии;
- удалении лицензии;
- количестве досье, загруженных в Систему на данный момент;
- возможной нехватке места на жестком диске;
- скором истечении срока действия пароля.

8 Настройки автоматического удаления событий Data Discovery в Traffic Monitor

Traffic Monitor применяет к событиям Data Discovery специальный antigarbage-фильтр. **По умолчанию** фильтр удаляет события Data Discovery, на которые не сработали политики Traffic Monitor или в которых не найдены объекты защиты.

Удаление событий Data Discovery можно настроить в конфигурационном файле `/opt/iw/tm5/etc/luaengined.conf`.

Режимы работы antigarbage-фильтра определяются параметром `DeleteDDEventsWithoutPolicy`:

- `true` - сохранять в базе данных Traffic Monitor только события, на которые сработали политики;
- `false` (значение по умолчанию) - сохранять события, которые содержат объект защиты или на которые сработали политики.

Чтобы antigarbage-фильтр не удалял события Data Discovery, укажите в параметре `DisableDeleteDDEventsForServers` серверы Data Discovery, для которых нужно сделать исключение.

Чтобы применить изменения:

1. Сохраните файл.
2. Перезапустите службу `iw_luaengined`:

```
iwtm restart luaengined
```

Пример:
Вы хотите, чтобы antigarbage-фильтр не применялся к событиям с серверов MainD и Dcompany, а для остальных серверов нужно сохранять только события, в которых сработали политики.

Значения параметров для конфигурационного файла luaengined.conf примера:

```
"DeleteDDEventsWithoutPolicy": true,
"DisableDeleteDDEventsForServers": ["MainD", "Dcompany"],
```

9 Ротация лог-файлов

9.1 Сервисы задач сканирования

Для выполнения задач сканирования Система использует сервисы: Puller, Sender, Ripper, CASI, Contents Processor, Task Execution Controller. Лог-файлы экземпляров сервисов хранятся в поддиректориях директории `/var/log/infowatch/disc` на сервере, где были запущены сервисы задачи сканирования.

При каждом запуске задачи Система добавляет в директорию `/var/log/infowatch/disc` поддиректорию для каждого экземпляра сервиса, участвующего в выполнении задачи. В поддиректорию добавляются лог-файлы экземпляра сервиса. Каждая поддиректория имеет уникальный идентификатор в ее названии.

9.2 Сервис Discoperator

Лог-файлы сервиса Discoperator хранятся в директории `/var/log/infowatch/disc` на ноде с Data Discovery, который установлен в режиме `central`. Сервис используется для работы веб-интерфейса.

Discoperator функционирует постоянно и добавляет записи в лог-файл. Если сервис был перезапущен, то Система добавляет в директорию `/var/log/infowatch/disc` поддиректорию для нового экземпляра сервиса.

9.3 Сервис TPS Agent

В директории `/var/log/infowatch/disc` на каждом сервере хранятся лог-файлы сервиса TPS Agent. Этот сервис используется для управления хранилищем сервера.

Сервис функционирует постоянно и добавляет записи в лог-файл. Если сервис был перезапущен, то Система добавляет в директорию `/var/log/infowatch/disc` поддиректорию для нового экземпляра сервиса.

9.4 Ротация лог-файлов

Экземпляры сервисов добавляют большое количество записей в лог-файлы. Размер лог-файлов постоянно растет, что приводит к уменьшению свободного дискового пространства.

Освободить дисковое пространство можно следующими способами:

- Остановить все задачи сканирования в Консоли управления, после чего удалить поддиректории и лог-файлы вручную из директории `/var/log/infowatch/disc`. При повторном запуске задачи Система:
  - создает новые поддиректории с новыми идентификаторами;
  - создает в поддиректориях лог-файлы, в которые будут добавляться записи о выполнении задачи.

> **Важно!**
>
> Если удалить лог-файлы у выполняющейся задачи, то записи не будут сохраняться в Системе, пока задача не будет остановлена и запущена повторно.

Важно!

Не рекомендуется удалять вручную директории и лог-файлы запущенных сервисов Discoperator и TPS Agent. Директории этих сервисов имеют имена вида:

- `discoperator-central-5c5769b58d-77rq2`
- `tps-agent-f85x8`

- Настроить ротацию лог-файлов.

Для регулярного и автоматического удаления устаревших записей рекомендуется настроить ротацию лог-файлов. Ротация лог-файлов – автоматический процесс для управления лог-файлами. При ротации в зависимости от настроек могут выполняться следующие действия:

- Создание нового файла, который является версией оригинального лог-файла. В новый файл перемещаются записи из оригинального лог-файла.
- Сжатие версий оригинального лог-файла.
- Удаление устаревших файлов.

9.5 Настройка ротации с помощью logrotate и crontab

Настройка ротации требуется на каждом сервере Data Discovery.

Чтобы настроить ротацию лог-файлов на сервере:

Важно!

Все действия необходимо выполнять от имени пользователя с правами root.

1. Настройте утилиту **logrotate**:
   a. Проверьте содержимое конфигурационного файла **`/etc/logrotate.conf`**
   Конфигурационный файл должен содержать следующую строку:

   ```
   include /etc/logrotate.d
   ```

   Добавьте указанную строку в конфигурационный файл, если строка отсутствует.
   b. В директории **`/etc/logrotate.d`** создайте файл для конфигурации logrotate для Data Discovery (в нашем примере имя файла – **`iwdd`**).
   c. Откройте созданный файл для редактирования и укажите в файле следующую конфигурацию:

   iwdd

   ```
   /var/log/infowatch/disc/*/*.log {
       daily
       copytruncate
       rotate 7
       notifempty
   ```

```
    compress
    missingok
}
```

Описание конфигурации

Содержимое	Описание
/var/log/infowatch/disc/*/*.log {	производить ротацию лог-файлов в поддиректориях директории `/var/log/infowatch/disc`
daily	производить ротацию ежедневно
copytruncate	во время каждой ротации создавать версию для каждого оригинального лог-файла, после чего перемещать все записи из оригинального файла в созданную версию
rotate 7	для каждого оригинального лог-файла хранить 7 последних версий, удалять более старые версии лог-файла
notifempty	не производить ротацию, если в оригинальном лог-файле нет записей
compress	производить сжатие каждой версии оригинального лог-файла
missingok	не сообщать об ошибке, если оригинальный лог-файл не был обнаружен
}	

d. Сохраните внесенные изменения. По умолчанию logrotate запускается автоматически.
e. Чтобы проверить корректность конфигурации без проведения ротации, выполните команду:

```
logrotate -d /etc/logrotate.d/iwdd
```

2. Если экземпляр сервиса был перезапущен, то новый экземпляр добавляет записи в новый лог-файл в новой поддиректории. Старый файл после одной ротации станет пустым и больше не будет подлежать ротации. Настройте автоматическое удаление неиспользуемых файлов и поддиректорий с помощью файла **crontab**:
   a. Откройте для редактирования файл `crontab` для пользователя root, выполнив команду:

```
crontab -u root -e
```

   b. Добавьте в конфигурационный файл одну строку:

```
30 5 * * * find /var/log/infowatch/disc/ -mtime +7 -name "*.log*" -delete > /dev/
null 2>&1; find /var/log/infowatch/disc/ -empty -type d -delete > /dev/null 2>&1
```

Указанный скрипт выполняется ежедневно в 5:30. Скрипт последовательно выполняет следующие действия:

i. Удаляет из поддиректорий лог-файлы и версии лог-файлов, которые были изменены более 7 дней назад.
ii. Удаляет пустые поддиректории.

c. Сохраните изменения. Скрипт будет автоматически запускаться ежедневно с помощью cron.

В результате настройки:

- logrotate регулярно осуществляет ротацию лог-файлов Data Discovery и удаляет устаревшие версии лог-файлов;
- скрипт, указанный в crontab, регулярно удаляет неиспользуемые файлы и пустые поддиректории.

10 Добавление пользовательского сертификата

Чтобы не допустить несанкционированный доступ к Системе и повысить защищенность канала передачи данных, можно добавить новый пользовательский сертификат для web-службы. Это действие доступно в любой момент использования Системы и выполняется через командную строку. Чтобы добавить пользовательский сертификат:

1. Разместите на диске два файла в формате PEM:
   - файл с сертификатом (например: `test.crt`);
   - файл с закрытым ключом (например: `test.key`).
2. Перейдите в директорию, в которую был распакован архив с дистрибутивом при установке Системы.
3. Выполните команду от имени пользователя с правами root:

   ```
   ./setup.py setwebkeys --certificate=/folder/test.crt --privatekey=/folder/test.key
   ```

   В нашем примере:
   - `/folder/test.crt` – полный путь к файлу с сертификатом;
   - `/folder/test.key` – полный путь к файлу с закрытым ключом.

Последний добавленный сертификат считается действительным. После добавления или замены сертификата обновите вручную все открытые вкладки браузера, используемые Системой.