SAFETICA ONE

Полная документация

Продукт: Safetica ONE
Версия: 10
Разработчик: Safetica Technologies

Более подробная информация размещена на сайте www.esetnod32.ru
Опубликовано: 2021

Содержание

Содержание 3
1. Введение 5
2. О Safetica 5
2.1. Продукты и модули Safetica 5
2.2. Архитектура 7
3. Установка 9
3.1 Автоматическая установка 9
3.2 Ручная установка 10
3.2.1. Перед установкой 10
3.2.2. Установка сервера 11
3.2.3. Установка консоли 19
3.2.4. Исходная конфигурация 21
3.2.5. Установка клиента 19
4. Консоль 27
4.1. Описание интерфейса 28
4.2. Режим настроек 31
4.3. Режим визуализации 35
4.4. Управление и настройки 39
4.4.1. Dashboard 39
4.4.2. Предупреждения 40
4.4.3. Отчеты 43
4.4.4. Обслуживание 46
4.4.4.1. Обзор конечных точек 46
4.4.4.2. Обновление и развертыввание 47
4.4.4.3. Деактивация рабочего места 51
4.4.4.4. Настройки интеграции 53
4.4.4.5. Настройки клиента 57
4.4.4.6. Сбор отладочной информации 60
4.4.4.7. Управление базой данных 62
4.4.4.8. Управление доступом 67
4.4.4.9. Менеджер лицензий 69
4.4.4.10. Категории 70
4.4.4.11. Активность пользователей 71
4.4.4.12. Переадресация клиента на другой сервер 73
4.4.4.13. Защита от неавторизованных действий с клиентом Safetica 74
4.4.5. Профиль 75
4.4.5.1. Настройки сервера 76

4.5. Safetica Discovery 80
4.5.1. Настройки функций 80
4.5.2. Устройства 82
4.5.3. Печать 82
4.5.4. Сетевой трафик 83
4.5.5. E-mails 84
4.5.6. Файлы 85
4.6. Safetica Protection 87
4.6.1. Журналы DLP 88
4.6.2. Правила DLP 89
4.6.3. Категории данных 91
4.6.3.1. Конфиденциальные данные 93
4.6.3.2. Существующие классификации 95
4.6.3.3. Контекстные правила 96
4.6.4. Зоны 99
4.6.5. Защита диска 105
4.6.6. Контроль устройств 107
4.6.7. Устройства BitLocker 110
4.6.8. Диски BitLocker 111
5. Клиент 113
5.1. Диалоги оповещений 113

1. Введение

Уважаемый пользователь!

Благодарим вас за выбор Safetica. В этом документе вы найдете подробное описание всех компонентов продукта и руководство по использованию отдельных функций. Вы познакомитесь с деталями процессов начиная с установки и начального развертывания в сети организации до совместного использования, оценки результатов и решения распространенных проблем.

Если предоставленная здесь информация не поможет решить проблему, свяжитесь с нашей службой технической поддержки https://www.esetnod32.ru/support/

Safetica предлагает новый подход к внутренней безопасности. Это единственное зрелое решение для защиты данных, разработанное с учетом масштабируемости и потребностей малых и средних компаний и крупного бизнеса. Решение предлагает защиту данных и один из лучших на рынке показателей времени окупаемости.

Safetica позволяет выйти за рамки «классической» защиты от потери данных с помощью целостного анализа поведения, который позволяет обнаруживать внутренние угрозы заблаговременно и реагировать до непосредственного инцидента. Решение предоставляет аналитические данные о рабочей среде компании, цифровых активах и операциях для оптимизации затрат. Никакие другие программные приложения не предлагают комплексный подход к защите от основных внутренних угроз.

Чтобы узнать, как устанавливать программное обеспечение, прочтите *Руководство по установке Safetica*. Чтобы быстро ознакомиться с основными методами и их использованием, воспользуйтесь *кратким руководством Safetica*.

2. О Safetica

Safetica – комплексное решение для защиты от утечек данных и от внутренних угроз, которое помогает выявлять риски безопасности, управлять потоком данных и защищать конфиденциальную информацию компании, а также соответствовать законодательным требованиям в области защиты данных. Информация о нарушениях безопасности передается с помощью мгновенных предупреждений и настраиваемых отчетов.

Safetica проста в развертывании и доступна по цене для компании любого масштаба. Более подробную информацию о продуктах и модулях можно найти на сайте www.esetnod32.ru или в базе знаний Safetica.

2.1. Продукты и модули Safetica

В портфеле Safetica три основных продукта и два дополнительных модуля.

Продукты

Safetica Discovery

Safetica Discovery предназначен для аудита безопасности операций с файлами и их передачи. Продукт помогает обнаруживать подозрительные действия, лучше понимать процессы безопасности и картину происходящего внутри организации.

Safetica Protection

Safetica Protection позволяет использовать гибкие политики DLP для защиты данных и предотвращения утечек важных файлов на различных устройствах и платформах. В распоряжении заказчика шифрование BitLocker и зонирование Safetica.

Safetica Enterprise

Safetica Enterprise поддерживает дополнительные функции, необходимые для крупных организаций. Продукт расширяет возможности DLP за счет автоматической интеграции с решениями сторонних производителей, поддержки нескольких доменов Active Directory и управления рабочим процессом. Есть возможность персонализировать приложение для конечных точек, добавив логотип заказчика.

Модули

Модули Safetica позволяют расширить возможности решения и закрыть большее число сценариев использования.

Safetica UEBA

Модуль анализа поведения пользователей и объектов оценивает действия пользователей и внутренние угрозы. Более подробная информация доступна в базе знаний Safetica.

Safetica Mobile

Решение для управления мобильными устройствами (MDM) предназначено для защиты данных на смартфонах и планшетов сотрудников. Более подробная информация доступна в базе знаний Safetica.

Устаревшие продукты

В качестве альтернативы предыдущему портфелю предлагаются следующие продукты:

- вместо Safetica Auditor – Safetica Discovery + Safetica UEBA
- вместо Safetica DLP – Safetica Protection + Safetica UEBA или Safetica Enterprise + Safetica UEBA (в зависимости от потребностей клиентов)
- вместо Safetica Supervisor – Safetica Discovery + Safetica UEBA. Более подробная информация об управлении приложениями и веб-контроле, об управлении печатью, а также о модуле Safetica Supervisor доступна по соответствующим ссылкам

2.2. Архитектура

Продукт Safetica основан на клиент-серверной архитектуре. Клиент Safetica на рабочих местах запускает коммуникацию с сервером. Вместе с клиентом на рабочих станциях запускается агент загрузчика, который предназначен для установки, обновления и управления другими клиентскими компонентами. Для управления, настройки и отображения полученных данных используется консоль управления или WebSafetica. Данные, полученные с отдельных рабочих мест, хранятся на сервере базы данных. База данных также хранит настройки всех компонентов Safetica.

Каждая из следующих частей может устанавливаться на отдельном компьютере.

Сервер

Сервер Safetica работает как служба на выделенном сервере, обеспечивая соединение между базой данных и другими компонентами Safetica и их дистанционное управление.

Рекомендуемое аппаратное и программное обеспечение

- четырехъядерный процессор 2,4 ГГц
- оперативная память 8 ГБ
- 100 ГБ места на диске
- общий или выделенный сервер, поддержка виртуальных машин или облачного хостинга
- требуется подключение к серверу MS SQL 2012 и выше или Azure SQL
- поддерживаемые операционные системы: Microsoft Windows Server 2012 и выше

Примечание. На одном компьютере может быть установлен только один экземпляр сервера.

Консоль

Консоль используется для настройки и управления клиентами и агентами загрузчика на рабочих местах, а также для серверных служб (размещенных на сервере) и баз данных. Кроме того, она служит для настройки функций Safetica на рабочих местах. Также она отображает выходные данные, статистику и графики. Может работать везде, где есть соединение с управляемым сервером.

Рекомендуемое аппаратное и программное обеспечение

См. требования к клиенту Safetica

WebSafetica

WebSafetica — веб-консоль для управления Safetica и отображения записей, полученных с рабочих мест. Более подробная информация о WebSafetica доступна в базе знаний.

Агент загрузчика

Агент загрузчика — компонент Safetica, используемый для управления клиентами

Safetica на конечных компьютерах. Он обеспечивает удаленную установку, обновление и выполняет другие задачи управления.

Рекомендуемое аппаратное и программное обеспечение

Агент загрузчика для Windows и macOS: см. требования к клиенту Safetica.

Клиент

Клиент обеспечивает все функции безопасности и мониторинга Safetica на конечных точках. *Клиентская служба* всегда запускается при запуске операционной системы и обеспечивает мониторинг, реализует политику безопасности и упрощает коммуникацию с базой данных и сервером.

В процессе установки клиента компонент *Агент загрузчика* будет установлен автоматически, если не был установлен раньше.

Клиент продолжает работать, даже если сервер недоступен (например, сервер не работает или клиент находится в другой сети). Он использует локальную зашифрованную и защищенную базу данных, где хранит все настройки и журналы до тех пор, пока снова не будет подключен к серверу.

Примечание. Минимальная поддерживаемая версия клиента Safetica — 9.0.

Рекомендуемое аппаратное и программное обеспечение

Для Windows:

- двухъядерный процессор 2,4 ГГц
- оперативная память 2 ГБ
- 10 ГБ места на диске
- поддерживаемые операционные системы: Microsoft Windows 7, 8.1, 10 (32-бит [x86] или 64-бит [x64])
- установочный пакет MSI
- .NET 4.7.2 и выше

Для macOS:

- четырехъядерный процессор 2,4 ГГц
- оперативная память 2 ГБ
- 10 ГБ места на диске
- поддерживаемые операционные системы: macOS 10.10 и выше (для использования всех функций Safetica Protection – macOS 10.15 и выше)

База данных

База данных используется для хранения настроек и записей, получаемых от всех компонентов Safetica.

Рекомендуемое аппаратное и программное обеспечение

- Microsoft SQL Server 2012 и выше, Microsoft SQL Express 2017 и выше, Azure SQL. MS SQL Express является частью универсального установщика и рекомендован для использования в диапазоне до 200 конечных точек.
- 200 ГБ места на диске (оптимально не менее 500 ГБ в зависимости от диапазона собираемых данных).
- Общий или выделенный сервер, поддержка виртуальных машин или облачного хостинга. База данных может быть размещена на одной машине с сервером Safetica.

Примечание. Требования к аппаратному и программному обеспечению для серверов баз данных, упомянутых выше, можно узнать на сайтах производителей. Более подробная информация доступна также в базе знаний.

3. Установка

Safetica устанавливается с помощью универсального инструмента установки, в который встроены все необходимые компоненты. После запуска инструмента установки вы сможете выбрать один из двух способов установки:

- Автоматическая установка (установка Safetica) — способ, при котором все компоненты автоматически устанавливаются на компьютер.
- Ручная установка (установка с извлечением компонентов) — ручной способ с выбором отдельных компонентов Safetica.

Выберите один из этих способов и продолжайте установку.

3.1 Автоматическая установка

После запуска установщика вы можете выбрать один из двух вариантов: *автоматическую* или *ручную* установку. В этом руководстве описывается только *автоматическая установка,* которая устанавливает компонент сервера, панели управления, в том числе WebSafetica, веб-сервер IIS и сервер баз данных Microsoft SQL Server Express на ваш компьютер. Клиентские программы будут установлены при первом запуске Safetica после ее установки. Убедитесь, что ваш компьютер достаточно мощный для работы с базой данных, сервером и WebSafetica. Рекомендуется следующая конфигурация: 4 ядра, 8 ГБ оперативной памяти, 100 ГБ места на диске. Эта способ установки предназначена предназначен исключительно для тестирования или для ограниченного числа клиентов Safetica, установленных на конечных компьютерах.

Если вы хотите изменить параметры установки или выполнить установку для большего числа клиентов, мы рекомендуем выбрать ручной способ установки. Описание этого способа доступно в полной версии руководства, которую можно открыть в установщике: *Ручная установка -> Документация -> Полное руководство*.

После запуска установщика Safetica выполните следующие действия:

1. Нажмите на вариант *Автоматическая установка* и примите условия лицензионного соглашения.
2. После этого вы увидите требования к аппаратному обеспечению. Прочтите их и продолжайте процесс установки.
3. Введите надежный пароль для базовой учетной записи администратора *safetica*. Примите условия лицензионного соглашения сервера SQL и запустите установку, нажав на кнопку *Установить*.

Примечание. WebSafetica использует веб-сервер Microsoft IIS и порты 80 и 443. Убедитесь, что на компьютере не запущено приложение, которое может заблокировать порты 80 или 443, либо настройте для IIS другие порты после установки.

3.2 Ручная установка

Для развертывания Safetica выполните следующую процедуру:

1. Перед установкой проверьте, соответствует ли ваша сеть условиям развертывания.
2. Установите сервер на выбранных компьютерах. В процессе установки выберите базу данных, которая будет использоваться сервером.
3. Установите консоль или WebSafetica на компьютере, с которого собираетесь управлять Safetica.
4. С помощью консоли подключитесь к серверу и настройте исходную конфигурацию Safetica.
5. Установите агент загрузчика на рабочих станциях.
6. С помощью консоли установите клиент на рабочих станциях (установка клиента через консоль возможна только на компьютерах с установленным агентом загрузчика).

После развертывания всех компонентов и проверки правильности установки вы можете начать работу с Safetica.

В следующей главе вы найдете более подробное описание каждого этапа развертывания.

3.2.1. Перед установкой

Перед установкой выполните следующие шаги:

1. Проверьте, выполняются ли требования к аппаратному и программному обеспечению для всех трех компонентов Safetica.
2. Проанализируйте свою корпоративную сеть:

- Решите, на какие компьютеры вы будете устанавливать сервер. При принятии этого решения учитывайте следующие аспекты:
    - Компьютер с сервером Safetica должен иметь возможность подключения к серверу SQL, на котором будут храниться основные базы данных.
    - С учетом количества одновременно подключаемых клиентов и типа используемого сервера базы данных расчитайте количество необходимых серверов для вашей среды. Допустимое количество клиентов, подключенных к одному серверу, ограничивается возможностями базы данных SQL, в которой этот сервер хранит данные (подробнее см. ниже).
- Решите, на какие компьютеры в вашей сети вы будете устанавливать консоль. Компьютеры с установленной консолью должны иметь возможность подключения ко всем серверам, которые вы собираетесь администрировать с помощью консоли управления.
- Решите, на какие компьютеры в вашей сети вы будете устанавливать агент загрузчика.
    - Компьютер с агентом загрузчика должен иметь подключение хотя бы к одному серверу Safetica.
- Решите, на какие компьютеры в вашей сети вы будете устанавливать клиент Safetica. При принятии этого решения учитывайте следующие аспекты:

- Для каждого клиента Safetica нужно решить, к какому серверу он будет подключаться. Клиент может быть подключен только к одному серверу единовременно.
- По этой причине компьютер с клиентом должен иметь подключение хотя бы к одному серверу в вашей среде.

- Выберите и назначьте серверы SQL, на которых будут храниться центральные базы данных каждого сервера. При принятии этого решения учитывайте следующие аспекты:
  - Каждому серверу требуются три выделенные базы данных на сервере SQL: одна для настроек, вторая для записей и третья для базы данных категорий.

3. Перед установкой компонентов Safetica (сервер, консоль, клиент) убедитесь, что процесс не будет блокироваться брандмауэром или антивирусными программами.

- Добавьте исключения для входящих соединений процесса STAService.exe и следующих портов на компьютерах, на которых будет установлен сервер:
  - 4438 (от клиента к серверу и базе данных).
  - 4441, 4442 (от консоли к серверу).
- Установите исключения для процесса STAConsole.exe на компьютерах, на которые будете устанавливать консоль:
- Установите исключения для следующих процессов на компьютерах, на которые будете устанавливать клиент: STCService.exe, STUserApp.exe, Safetica.exe, исходящие и входящие соединения.
- Установите исключения для порта 1433 (порт по умолчанию для связи с базой данных) на компьютерах, на которых вы собираетесь устанавливать базы данных.
  - 1433 (от клиента и сервера к базе данных).

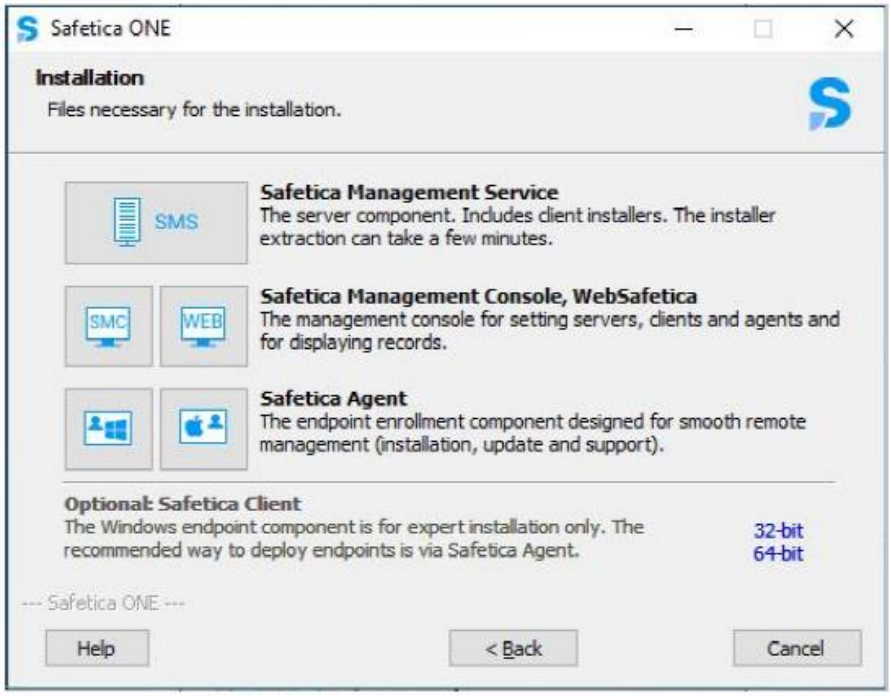
4. Загрузите универсальный установщик с последней версией Safetica.

- Универсальный установщик содержит все необходимые для установки компоненты.

3.2.2. Установка сервера

Сервер Safetica обеспечивает взаимное подключение всех клиентов Safetica, консоли и баз данных. Для установки выполните следующие действия:

1. Запустите универсальный установщик, который вы загрузили. Выбрав язык и приняв условия лицензионного соглашения, переходите к следующему пункту (*Установка -> Safetica Management Service*).



2. Установка. Здесь у вас есть несколько вариантов:

   - Запустить установку напрямую из универсального инструмента, нажав на Запустить установщик.
   - Извлечь только установщик сервера, который вы затем сможете использовать отдельно, для последующей установки.

   Примечание. В третьей части «Инструменты и компоненты» вы найдете перечень компонентов, необходимых для правильной установки клиента или Microsoft SQL Server 2017 Express. Если вы собираетесь устанавливать сервер Microsoft SQL Server 2017 Express с помощью этого установщика, убедитесь, что на вашем компьютере установлен компонент Microsoft Installer 4.5. Если этот компонент еще не установлен, установите его.

3. После запуска установщика (универсального или извлеченного ранее) снова выберите язык и примите условия лицензионного соглашения.

4. Выберите папку установки.

5. Затем нужно выполнить важный процесс настройки сервера Microsoft SQL Server, на котором установленный сервер будет хранить свои базы данных.

6. Также настройте следующие параметры:

   - *Включение автоматических обновлений определений*. Выбрав этот параметр, вы разрешаете консоли автоматически устанавливать обновления для определений (при наличии подключения к интернету и базе данных). Процесс обновления может увеличить нагрузку на сервер SQL Server. Эту настройку можно изменить в любой момент, открыв Консоль -> Обслуживание -> Обновление и развертывание -> Обновления определений.
   - *Автоматическая отправка статистики*. Выберите этот параметр, чтобы разрешить консоли отправлять анонимную статистическую информацию в Safetica Technologies, что поможет нам активно решать возникающие проблемы и улучшать продукт. Никакая конфиденциальная или связанная с безопасностью информация отправляться не будет. Эту настройку можно изменить в любой момент, открыв Консоль -> Обслуживание -> База данных -> Обслуживание -> Отправка статистики.

Рекомендуется разрешить оба варианта.

7. Завершите установку. Сервер установится и запустится автоматически.
8. После завершения установки проверьте, запустился ли файл STAService.exe Диспетчер задач -> Службы -> STAService — запущена.
9. И наконец, проверьте, добавили ли вы исключения в брандмауэр и антивирус для процесса STAService.exe, и не заблокированы ли порты 4438, 4441 и 4442.

Примечание. По умолчанию консоль использует порты 4441, 4442 для подключения к серверу, а клиент использует порт 4438. Вы можете изменить эти настройки, чтобы использовать другие порты.

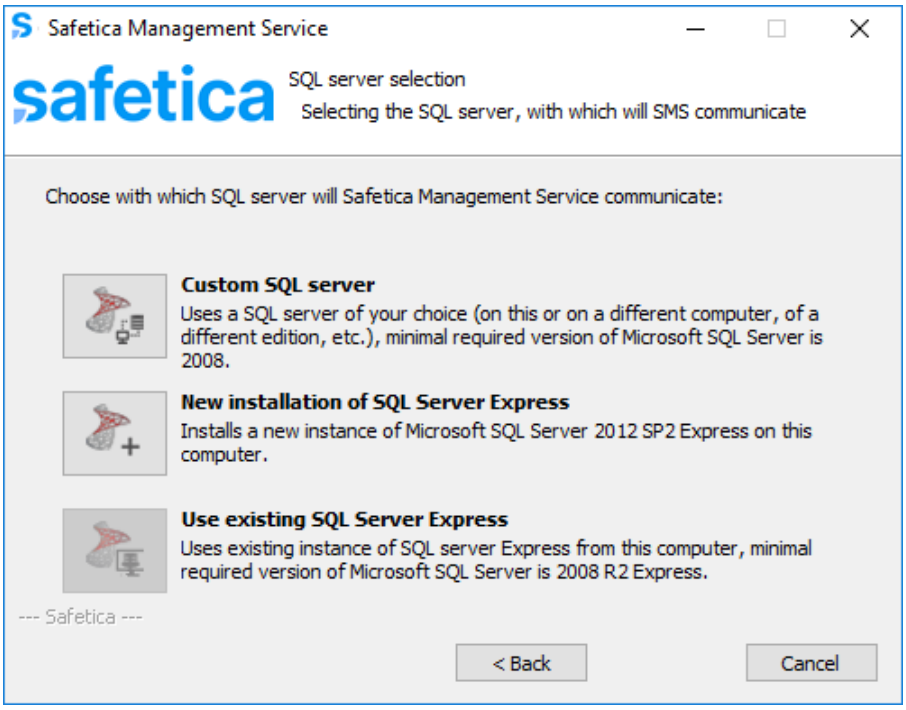
3.2.2.1. Настройки сервера Microsoft SQL Server

Теперь вы должны выбрать SQL Server, на котором сервер будет хранить базы данных. У вас есть несколько вариантов:

A. *Пользовательский сервер SQL Server.* Выбрав эту опцию, вы сможете создать базу данных в существующей системе Microsoft SQL Server. Поддерживаемые серверы Microsoft SQL Server перечислены в списке требований. Описание настройки приводится в разделе Настройка существующего сервера SQL Server.

B. *Новая установка SQL Server Express.* Выбрав этот вариант, вы установите сервер Microsoft SQL Server 2017 Express на ваш компьютер. Для создания баз данных сервера будет использоваться новый сервер. Описание установки приводится в разделе Установка нового сервера SQL Server Express.

C. *Использование существующего сервера SQL Server Express.* Если на компьютере, на который вы собираетесь установить сервер, уже есть экземпляр Microsoft SQL Server 2017 Express, вы можете выбрать этот вариант. Для хранения баз данных сервера будет использоваться существующий SQL Server. Описание настройки приводится в разделе Настройка существующего сервера SQL Server.



3.2.2.1.1. Настройка существующего сервера SQL

Если вы выбираете свой сервер SQL при установке сервера Safetica, вам нужно сначала проверить, правильно ли он настроен для хранения баз данных.

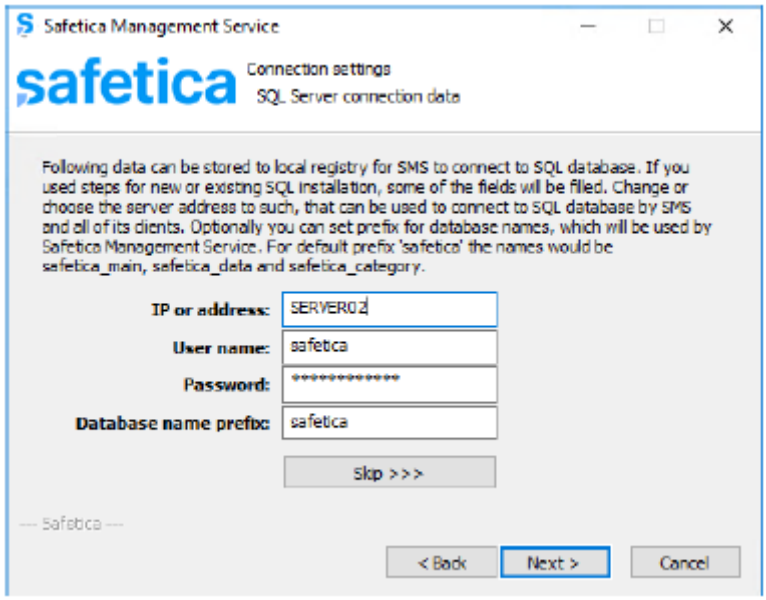
- Убедитесь, что для SQL Server настроен смешанный режим аутентификации, то есть одновременное использование аутентификации SQL Server и аутентификации Windows (откройте Microsoft SQL Server Management Studio -> Server settings - > Security -> SQL Server and Windows Authentication mode).
- Сервер SQL должен быть доступен в сети по протоколу TCP/IP (откройте SQL Server Configuration Manager -> SQL Server Network Configuration -> TCP/IP Enabled).
- На сервере SQL должен быть создан пользователь с правами администратора (*sysadmin*). Используйте этого пользователя при вводе данных.

Если у вас нет установленного сервера SQL, следуйте инструкциям и переходите к разделу Установка пользовательского сервера SQL Server.

Если сервер SQL Server уже установлен и соответствует всем описанным выше критериям, вы можете начать настройку:

1. Сначала внесите следующую информацию:

- *IP или адрес* - Введите IP-адрес или имя SQL Server. Сервер SQL должен быть доступен по этому адресу или имени как для вновь установленного сервера, так и для клиентов Safetica, которые будут подключаться через этот сервер. При заполнении этого раздела вы можете указать экземпляр SQL Server (например, 192.168.100.1\InstanceName). Если вы введете только IP-адрес или имя, будет применяться экземпляр сервера SQL по умолчанию.
- *Имя пользователя* - Введите имя пользователя для сервера SQL. Пользователь должен иметь права администратора (*sysadmin*). Этот пользователь будет использоваться при создании и подключении ко всем трем базам данных, которые будут автоматически созданы на сервере SQL после его установки.
- *Пароль* - Пароль пользователя сервера SQL.



- *Префикс имени базы данных* - Добавляет префикс перед именем базы данных. Например, при использовании префикса db имена баз данных будут выглядеть следующим образом: db_main, db_log и db_category

2. Нажмите *Проверить и сохранить*.

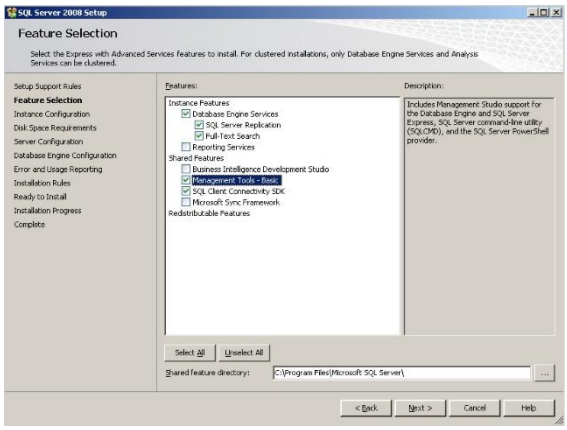
- Нажмите *Далее*, чтобы продолжить и завершить установку сервера. После завершения установки сервера на сервере SQL будет создана база данных safetica_data.

Вы можете изменить подключение к серверу с помощью консоли в разделе Настройки сервера. Настройка этого подключения описана в разделе настроек сервера.

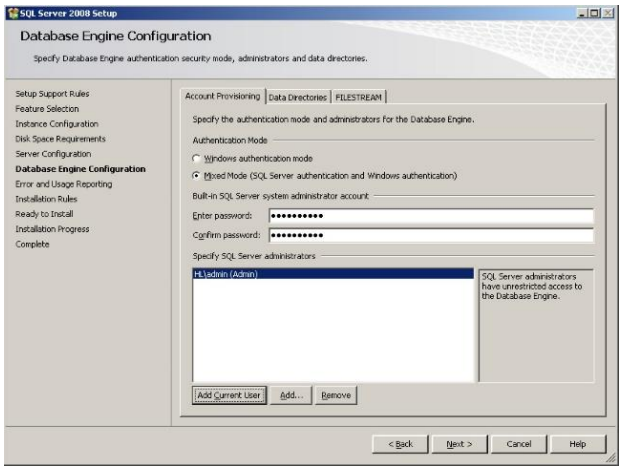
Установка сервера Microsoft SQL Server

Если у вас нет установленного сервера SQL, при установке нового SQL Server выполните следующие операции:

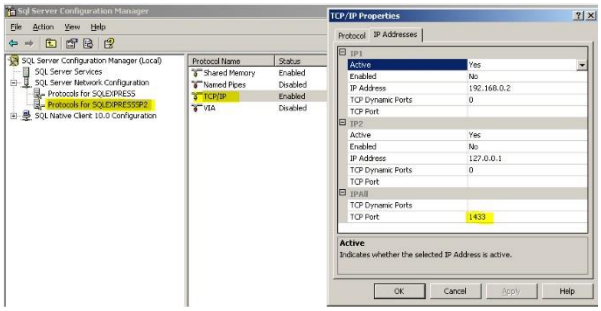
1. Установите MS SQL на свой сервер, используя следующие компоненты.



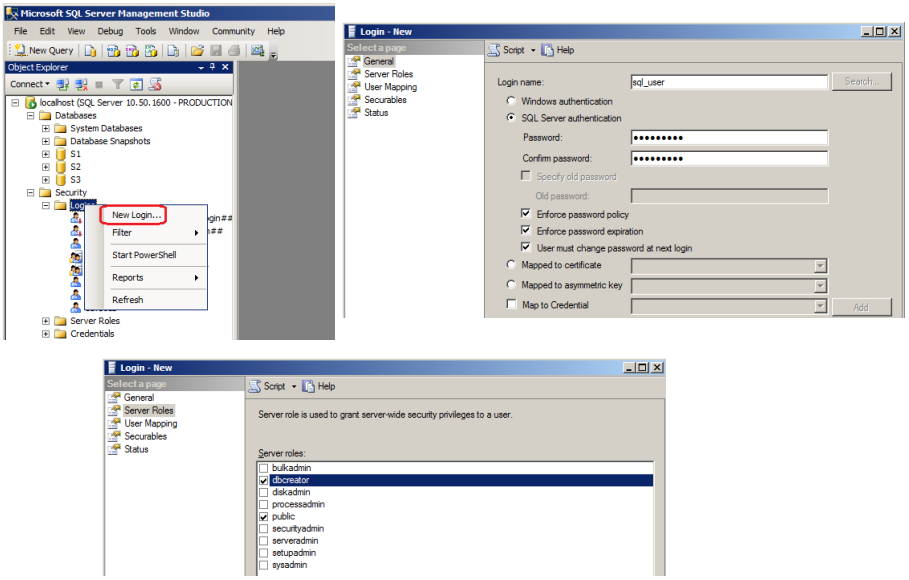
2. На соответствующем этапе установки настройте смешанный режим аутентификации.



3. Убедитесь, что сервер MS SQL настроен на прослушивание, например, порта 1433. Вы можете сделать это с помощью инструмента Sql Server Configuration Manager (Менеджер настройки SQL Server).



4. Создайте нового пользователя MS SQL с правами, позволяющими создавать базы данных через инструмент SQL Server Management Studio. В настройках выберите тип аутентификации «Аутентификация SQL Server» и введите новый пароль.



Подключение сервера к этим базам данных настраивается в консоли в разделе Настройки сервера.

3.2.2.1.2. Установка нового сервера SQL Server Express

Если у вас нет сервера SQL Server, вы можете установить Microsoft SQL Server 2017 Express из этого установщика. Обратите внимание на следующие ограничения:

- использует только один процессор.
- использует не более 1 ГБ оперативной памяти.
- максимальный размер базы данных — 10 ГБ.

Из-за ограничений к SQL Server Express максимальное числов клиентов (Safetica Endpoint Client) – 250.

При настройке нового сервера SQL Server по умолчанию вводятся следующие параметры:

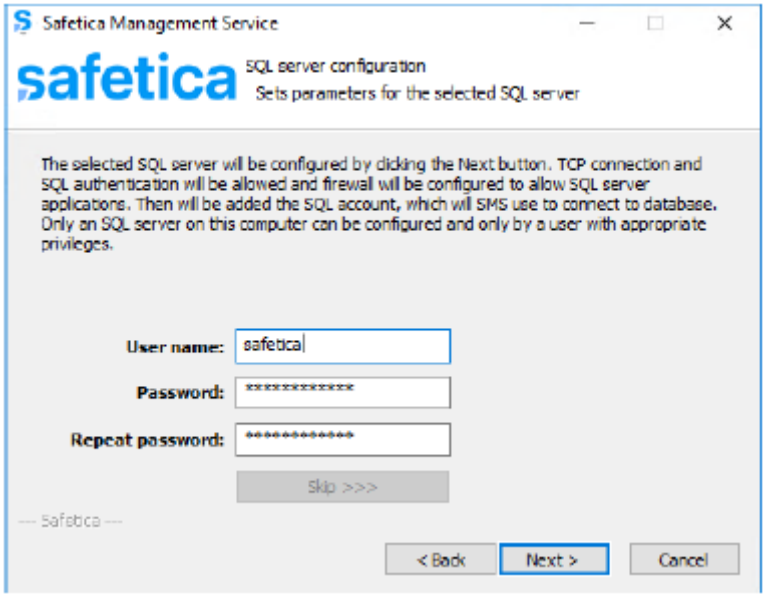
- имя экземпляра сервера SQL — MSSQLSERVER.
- для пользователя «sa» по умолчанию установлен пароль *S@fetic@2004*. Пользователь «sa» будет иметь доступ ко всем трем базам данных.

Примечание. Если групповая политика (локальная или политика домена) диктует определенную сложность пароля, то для установки SQL необходимо ввести пароль, соответствующий настроенной политике.

Нажав на кнопку *Использовать значения по умолчанию,* вы сможете изменить приведенные выше данные. Из соображений безопасности мы рекомендуем использовать другое имя для пользователя «*sa*».

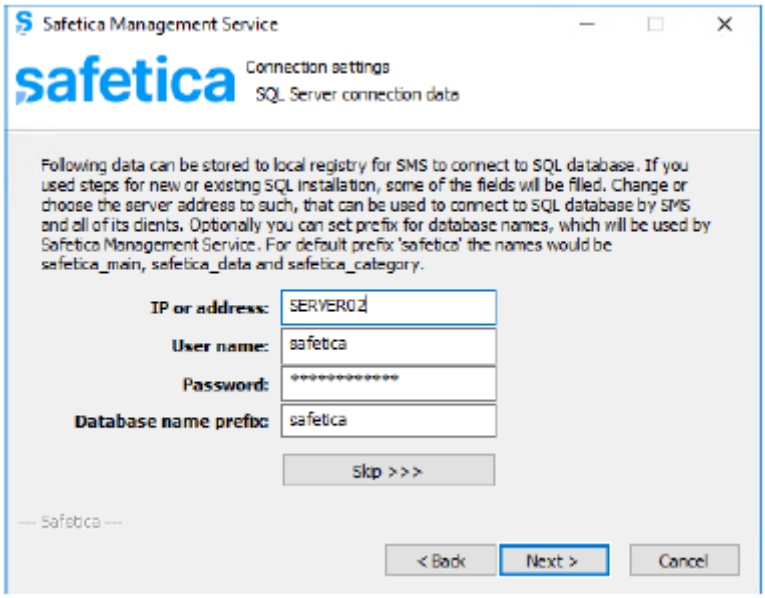
Приняв условия лицензионного соглашения Microsoft SQL Server 2017 Express, вы можете нажать *Далее*, чтобы начать установку сервера SQL.

После завершения установки сервера SQL Server Express нажмите Далее и введите имя пользователя и пароль сервера SQL, которые будут использоваться для доступа к базам данных. Пользователь по умолчанию — *safetica,* пароль — *S@fetic@2004*. Из соображений безопасности мы рекомендуем изменить пароль по умолчанию.



Нажмите Далее.

По завершении настройки сервера SQL Нажмите Далее и подтвердите настройки подключения сервера SQL в следующем диалоговом окне, нажав *Проверить и сохранить*. Нажмите *Далее.*



Продолжите процесс и завершите установку сервера. После успешной установки на сервере SQL будет создана база данных safetica_data.

Примечание. Впоследствии вы можете изменить подключение к серверу в разделе консоли Настройки сервера.

3.2.2.1.2. Настройка существующего сервера SQL Server Express

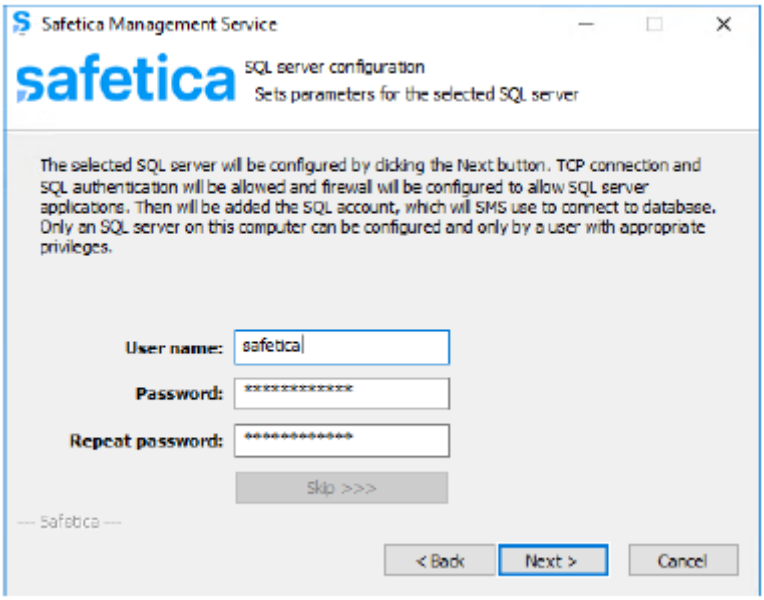
Если на компьютере, на который вы устанавливаете сервер, уже установлен сервер Microsoft SQL Server 2017 Express, вы можете использовать его для создания баз данных. Установщик автоматически перенастроит установленный на компьютере сервер SQL. Сервер автоматически подключится к этому экземпляру и после установки создаст соответствующие базы данных.

Примечание. Выпуск Express имеет следующие ограничения:

- использует только один процессор.
- использует не более 1 ГБ оперативной памяти.
- максимальный размер базы данных — 10 ГБ.

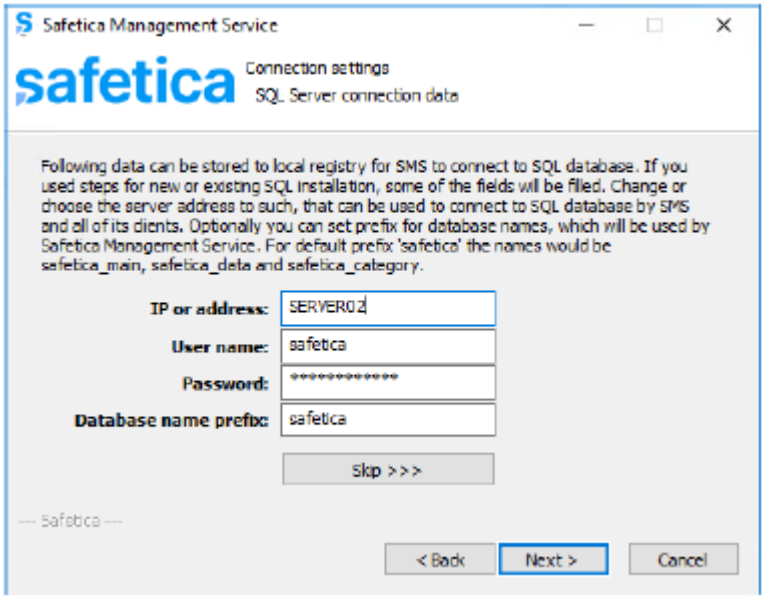
Из-за ограничений к SQL Server Express максимальное число клиентов (Safetica Endpoint Client) – 250.

В первом диалоговом окне введите имя пользователя и пароль сервера SQL, которые будут использоваться для доступа к базе данных. Пользователь по умолчанию — *safetica,* пароль — *S@fetic@2004*. Из соображений безопасности мы рекомендуем изменить пароль по умолчанию.



Нажмите Далее.

По завершении настройки сервера SQL Нажмите Далее и подтвердите настройки подключения сервера SQL в следующем диалоговом окне, нажав *Проверить и сохранить*. Нажмите *Далее*.



Продолжите процесс и завершите установку сервера. После успешной установки на сервере SQL будет создана база данных safetica_data.

Примечание. Впоследствии вы можете изменить подключение к серверу в разделе консоли Настройки сервера.

3.2.3. Установка консоли

Консоль представляет собой центральный пульт управления программным обеспечением. Она используется для настройки и управления клиентами и серверами, а также для управления базами данных и, конечно же, для управления модулями Safetica. В консоли также отображаются статистика, диаграммы и результаты мониторинга. С помощью консоли вы можете управлять несколькими экземплярами серверов Safetica. Вам нужно только запустить консоль на любом из компьютеров, имеющих доступ к управляемому серверу. Лицензия не ограничивает количество установок консоли или количество ее пользователей.

Продолжайте установку следующим образом:

1. Запустите универсальный установщик, который вы загрузили ранее. Выбрав язык и приняв условия лицензионного соглашения, переходите к пункту *Установка > Safetica Management Console*.
2. Здесь у вас есть несколько вариантов:

- Запустить установку напрямую из универсального инструмента, нажав на кнопку *Запустить установщик*.
- Извлечь только установщик консоли, который вы затем сможете использовать отдельно для последующей установки.

  Примечание. В третьей части «Инструменты и компоненты» вы найдете перечень компонентов, необходимых для правильной работы клиента Safetica или Microsoft SQL Server 2017 Express.

3. После запуска установщика (универсального или извлеченного ранее) снова выберите язык и примите условия лицензионного соглашения. Выберите папку установки и завершите установку.
4. В конце проверьте, добавили ли вы исключения в брандмауэр и антивирус для процесса *STAConsole.exe*.

3.2.4. Установка клиента

Клиент Safetica — последний из компонентов продукта Safetica, который вам нужно установить. Это важный компонент. На клиентских компьютерах он обеспечивает выполнение политик безопасности и правильную работу всех функций, настроенных на консоли. В нем также можно настроить набор инструментов безопасности для конечных пользователей.

Рекомендованная процедура установки

1. Установите агент загрузчика на конечной рабочей станции.
2. Установка клиента Safetica выполняется удаленно через *Консоль -> Обслуживание -> Управление конечной точкой*. Следуйте инструкциям, содержащимся в разделе *Управление конечной точкой.*

Ручная установка с использованием универсального установщика

1. Запустите универсальный установщик, который вы загрузили ранее. После выбора языка и

подтверждения лицензионных условий перейдите в раздел *Установка > Safetica Endpoint Client x86 или x64* в зависимости от версии операционной системы, установленной на рабочей станции.

2. Здесь у вас есть несколько вариантов:

- Запустить установку напрямую из универсального инструмента, нажав на кнопку *Запустить установщик*.
- Извлечь только установщик клиента, который вы затем сможете использовать отдельно для последующей установки.

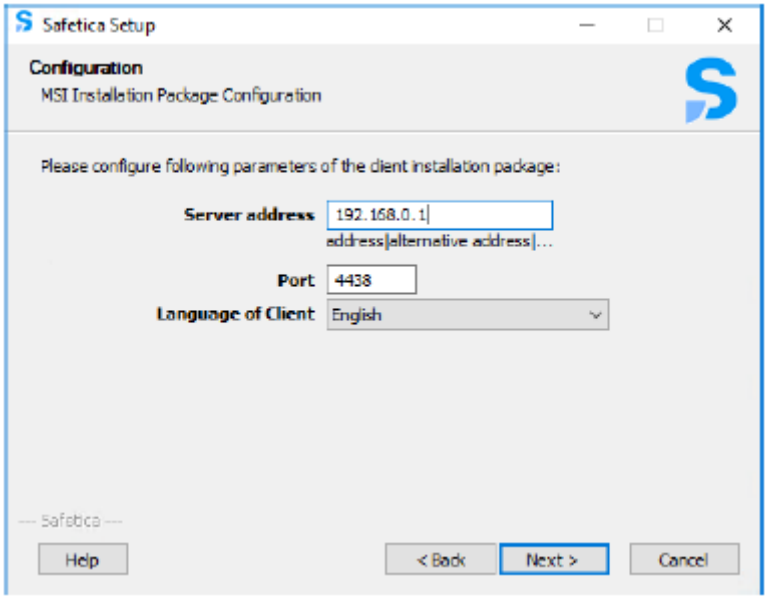
  Примечание. В третьей части «Инструменты и компоненты» вы найдете перечень компонентов, необходимых для правильной работы клиента Safetica или Microsoft SQL Server 2017 Express.

3. Перед извлечением или запуском установщика вас попросят ввести следующую информацию:

- *Адрес сервера* — адрес сервера, к которому подключается клиент.

  Примечание. Вы можете ввести несколько адресов, которые клиент сможет использовать для подключения к одному серверу. Это полезно для сценариев, в которых клиент устанавливается на ноутбуке, используемом в том числе вне помещений компании, где у него будет другой адрес для подключения к серверу. При вводе нескольких адресов разделяйте их символом |. Пример: 192.168.100.2|158.142.12.10|145.65.87.22.

- *Порт* — порт, который прослушивается сервером. По умолчанию это порт 4438.
- *Язык клиента* — язык клиента.



4. Выберите папку установки.

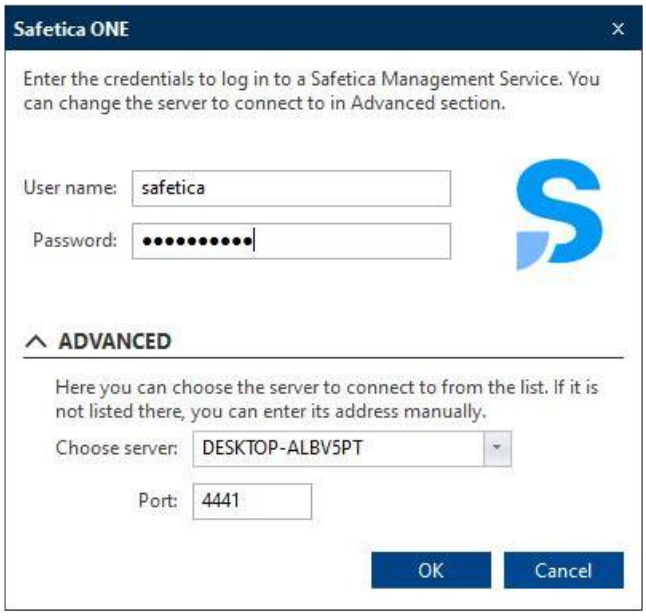
5. Вы можете проверить успешность установки из консоли, где вы найдете пиктограмму в дереве пользователей рядом с именем рабочего места. Если вы не можете найти в консоли конечную рабочую станцию, проверьте, запущена ли на ней служба STCService.exe Диспетчер задач Windows > Службы > STCService — запущена) и убедитесь, что вы добавили в брандмауэр и антивирус исключения для следующих процессов: STCService.exe, STPCLock.exe, STMonitor.exe, STUserApp.exe, and Safetica.exe.

3.3. Исходная конфигурация

После успешной установки консоли и сервера нужно правильно настроить всю систему до начала установки агента загрузчика и клиента на конечных компьютерах. Все действия по администрированию и настройке выполняются через консоль.

Обзор основных этапов настройки:

1. Запустите консоль. В диалоговом окне введите реквизиты служебной учетной записи, чтобы войти на сервер. Имя служебной учетной записи — *safetica,* а пароль по умолчанию — *S@fetic@2004*. В расширенных настройках введите адрес или имя сервера, на котором установлен сервер. Используйте порт по умолчанию 4441 для входа в консоль на сервере. Нажмите OK для подтверждения.



2. После запуска Safetica Management Console откроется мастер первичной настройки. На втором этапе вы можете добавить собственный SMTP сервер, чтобы получать уведомления и отчеты Safetica.

3. На третьем этапе вы можете изменить пароль служебной учетной записи Safetica для входа в консоль Safetica. Нажмите *Далее*.

   Примечание. Служебная учетная запись имеет все права для работы с функциями и настройками Safetica. Данные для входа в эту учетную запись следует хранить в надежном месте. Если вы хотите предоставить другим пользователям доступ к Safetica, создайте для них новую учетную запись на вкладке Обслуживание -> Управление доступом -> Добавить аккаунт.

4. На четвертом этапе вы можете импортировать в Safetica корпоративную структуру из Active Directory. Это возможно, только если компьютер с сервером Safetica находится в домене. Если вы не используете эту опцию, новые подключенные клиенты будут помещены в группу Неизвестные. Также вы можете выполнить импорт из Active Directory позднее, выбрав *Профиль -> Настройки сервера* в разделе *Настройки соединения с базой данных*.

5. Этот шаг поможет вам установить агент загрузчика на конечных компьютерах, чтобы их можно было подключить к Safetica. Нажав Получить пакет Агента, вы запустите создание агента загрузчика, который затем можно будет установить на всех рабочих станциях. Установить агент можно двумя способами:

   - удаленная (пакетная) установка;

- ручная установка.

После установки агентов загрузчика вы можете автоматически установить и активировать клиенты Safetica, нажав *Автоматическая регистрация конечных компьютеров*. Задачей установки клиента можно управлять из меню *Консоль -> Обслуживание -> Управление конечной точкой*

6. На шестом шаге введите лицензионный ключ Safetica. Лицензионный ключ можно ввести позднее, открыв меню *Обслуживание -> Менеджер лицензий*. Функции Safetica не будут доступны без лицензионного ключа.
7. Седьмой шаг – введите название компании и email, на который будут направляться уведомления Safetica.
8. Определите зону электронной почты компании и укажите правила контента для описания конфиденциальных данных. Вы можете выбрать ID, номера кредитных карт и др. На этом этапе можно включить блокировку опасных категорий веб-сайтов и приложений (вредоносное ПО, клавиатурные шпионы, майнеры и т. д.).

   По умолчанию мониторинг приложений, веб-сайтов, сетевого трафика, устройств и печати включен.
9. Поздравляем! Продукт настроен и готов к защите данных.

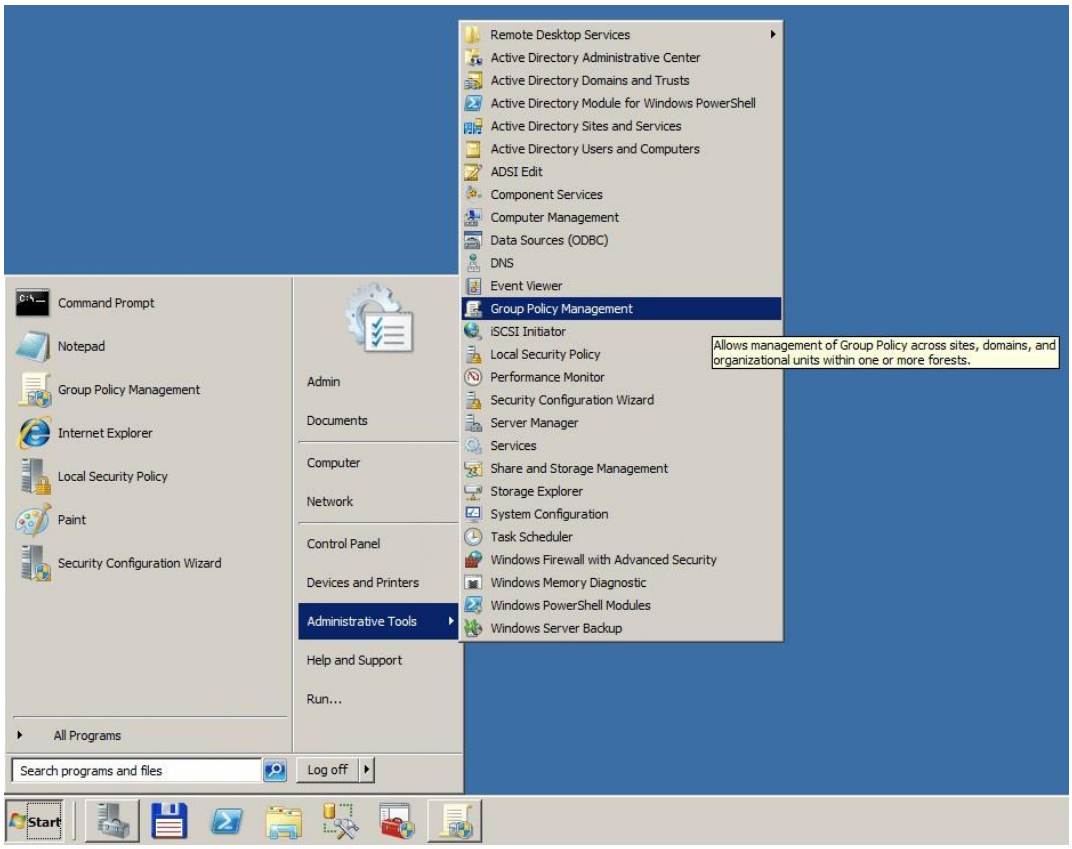
Все настройки можно просмотреть и изменить в консоли после завершения работы мастера начальной установки.

3.3.1. Пакетная установка агента Safetica с помощью GPO

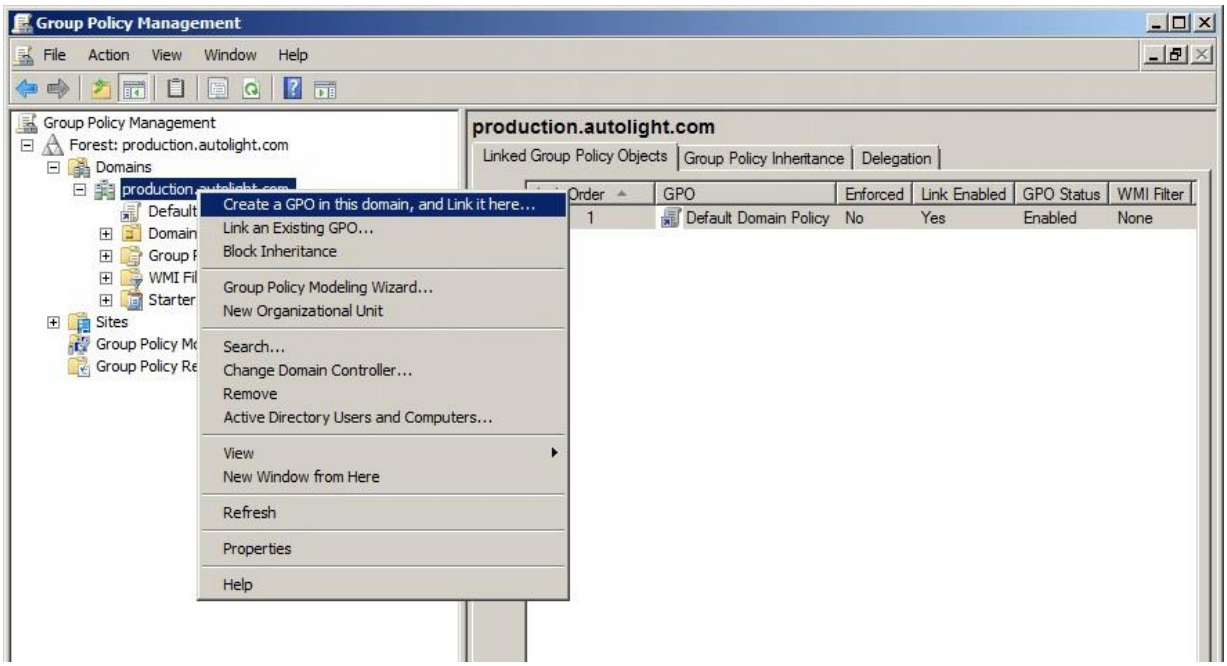
Если вы используете Active Directory, агент установщика можно установить в массовом режиме через групповую политику. Чтобы использовать массовую установку, необходимо извлечь соответствующий пакет MSI компонента агента Safetica из универсального пакета.

Установка будет описана на примере установки с использованием групповой политики в Windows Server 2008 R2. Описанные имена и некоторые шаги могут несколько отличаться в зависимости от версии серверной системы.

1. Запустите универсальный установщик Safetica.
2. Перейдите в *Установка -> Агент Safetica -> Извлечь установщик*. В конфигурации установщика введите адрес сервера и порт, к которому будет подключаться агент загрузчика. Сохраните пакет установки на общем диске или в общем каталоге в корпоративной сети и установите права доступа (будет достаточно прав на чтение и запуск) к этой папке для выбранной группы (например, по умолчанию — для *пользователей домена* и *компьютеров домена*).
3. Перейдите в *Administrative Tools -> Group Policy Management.*

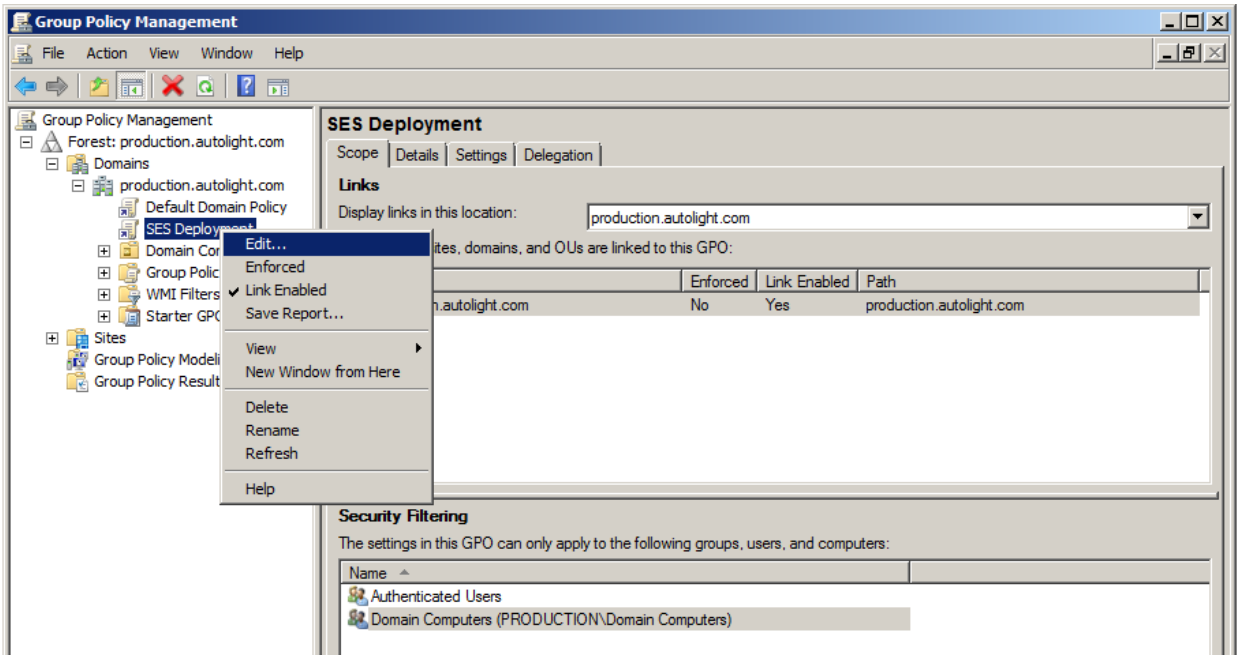


4. Щелкните правой кнопкой мыши на организационном подразделении, в котором вы хотите развернуть агент загрузчика, и выберите *Create a GPO in this domain and link it here ...*

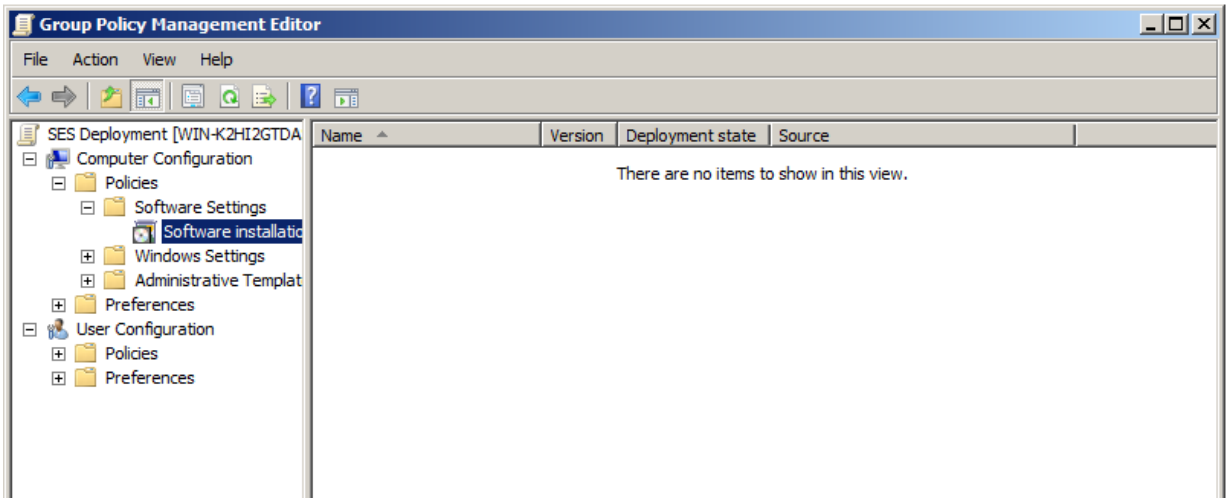


5. Дайте произвольное имя новому объекту (например, Safetica Deployment).

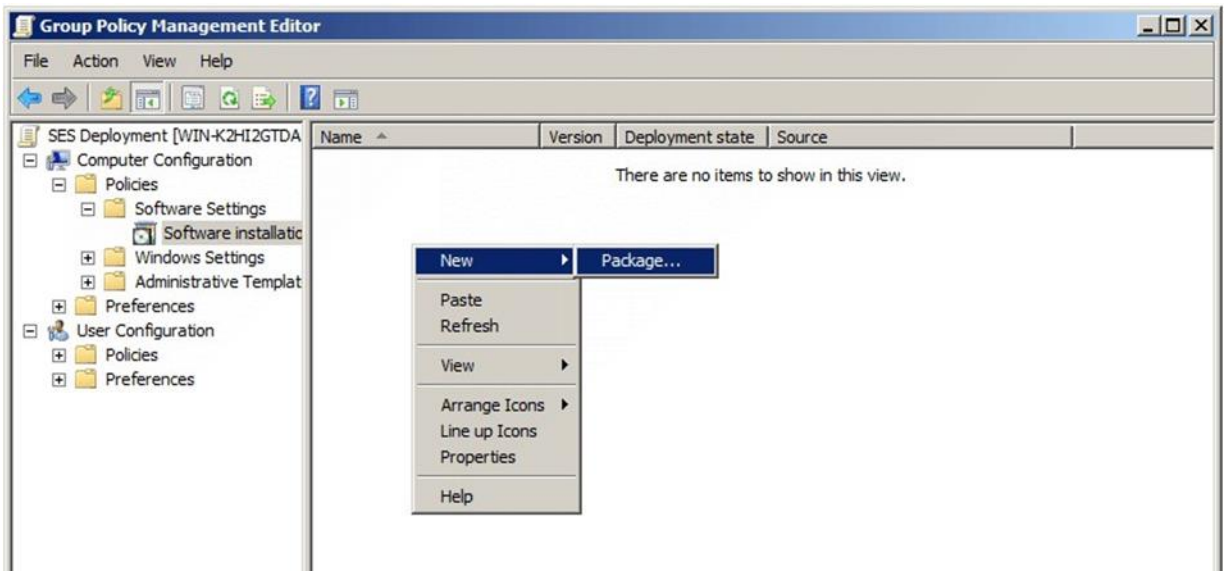
6. Выберите вновь созданную вами групповую политику и щелкните правой кнопкой мыши, чтобы выбрать Edit.



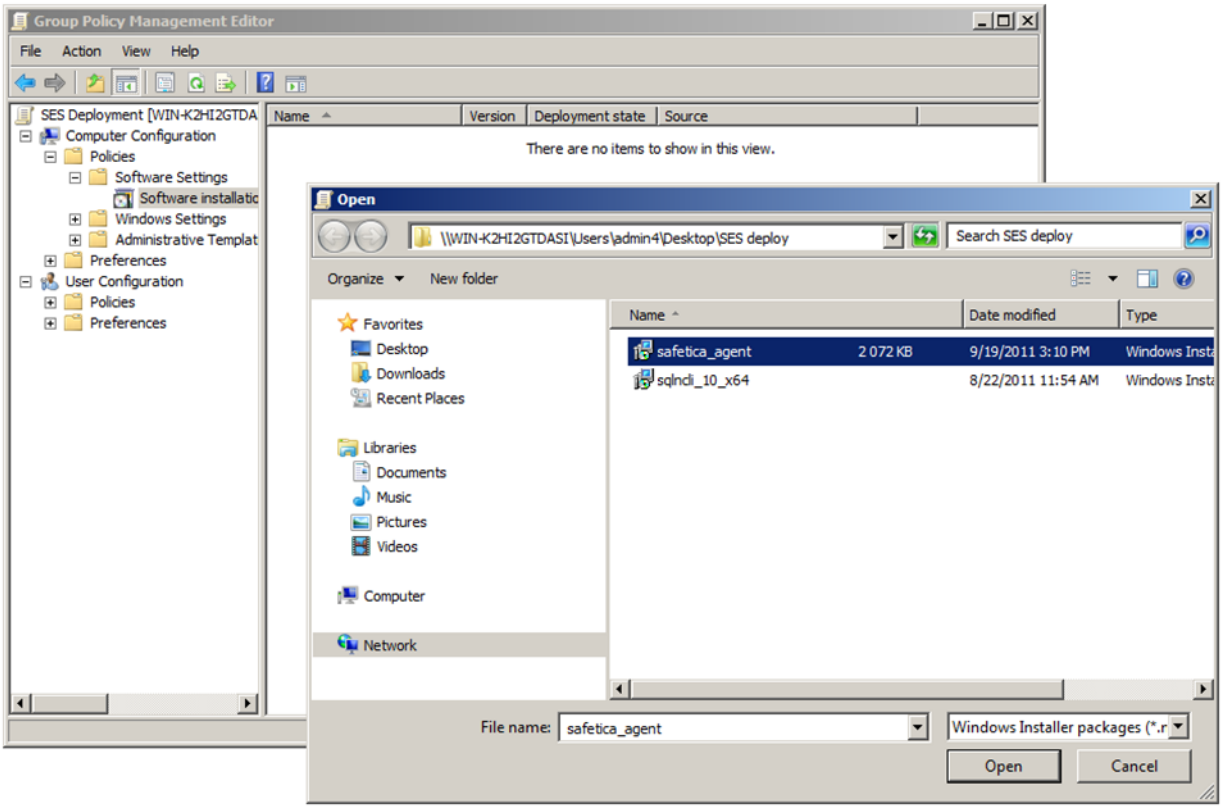
7. В открывшемся окне перейдите к *Computer Configuration -> Policies -> Software Settings* и выберите *Software installation.*



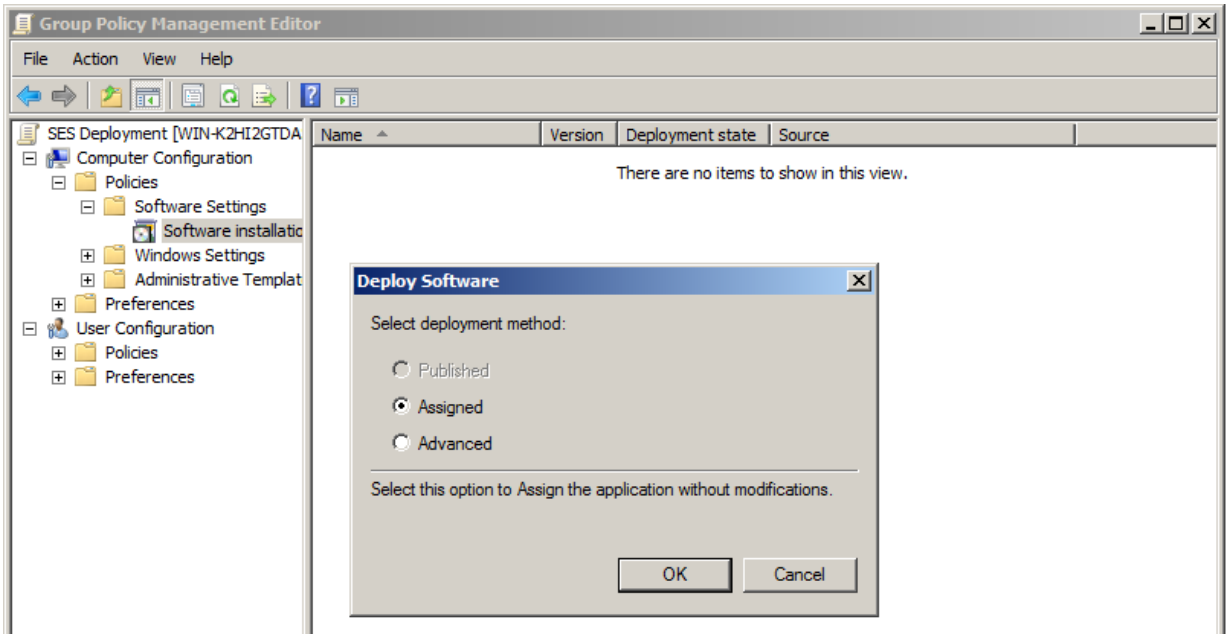
8. Щелкните правой кнопкой мыши на окне со списком программного обеспечения и выберите New Item -> *Package..*



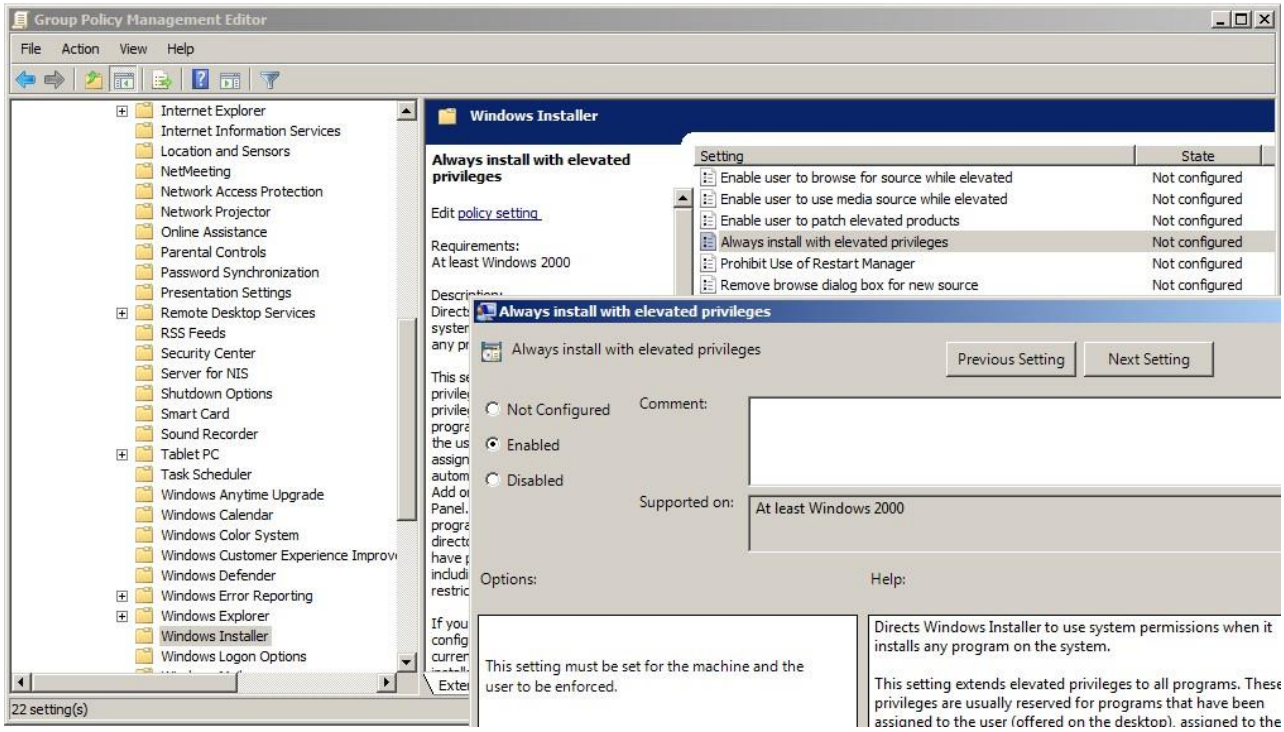
9. В диалоговом окне выбора пакета MSI перейдите в общую сетевую папку, в которую вы скопировали пакет MSI с агентом загрузчика, и выберите его.



10. В следующем диалоговом окне выберите Assigned и подтвердите выбор.



11. Затем откройте *Computer Setup -> Management Templates -> Windows Components -> Windows Installer.* Там найдите элемент *Always install with elevated privileges* и установите для него значение *Enabled*. Это гарантирует, что агент загрузчика правильно и без проблем будет установлен на конечных рабочих станциях.



12. Агент загрузчика будет автоматически установлен после перезагрузки клиентских компьютеров, для которых была создана политика. Чтобы обеспечить обновление политики, введите команду *gpupdate/force на клиентской рабочей станции*.

13. На этом конфигурация политики завершена, а дистрибутив агента загрузчика готов к установке. При запуске клиентских компьютеров агент загрузчика будет установлен на них.

3.3.2. Ручная установка агента загрузчика

Агент загрузчика используется для установки, обновления и управления клиентом Safetica на конечных рабочих станциях. Для ручной установки агента загрузчика на конечной рабочей станции выполните следующие действия:

1. Откройте универсальный установщик и выберите свой язык. Подтвердите условия лицензии и перейдите в *Установка > Агент Safetica.*
2. Здесь у вас есть несколько вариантов:

- Запустите установку напрямую из универсального установщика, нажав кнопку Запустить установщик.
- Извлеките только установщик агента загрузчика, который вы можете использовать отдельно для последующих установок.

  Примечание. В третьей части «Инструменты и компоненты» вы найдете перечень компонентов, необходимых для правильной установки клиента или Microsoft SQL Server.

3. На следующем шаге для правильного подключения загрузчика к серверу внесите следующую информацию:

- *Адрес сервера* — адрес сервера, к которому будет подключаться агент загрузчика.

  Примечание. Также вы можете ввести несколько адресов, которые могут использоваться агентом загрузчика *для подключения к серверу. Это полезно для сценариев, в которых агент загрузчика устанавливается на ноутбуке, используемом в том числе вне помещений компании, где у него будет другой адрес для подключения к серверу. При вводе нескольких адресов разделяйте их символом |. Пример: 192.168.100.2|158.142.12.10|145.65.87.22.*

- *Порт* — порт, который будет прослушиваться сервером. По умолчанию это порт 4438.

  Нажмите Далее.

4. После сохранения настроек запустится установщик агента загрузчика. После нажатия кнопки *Далее* агент загрузчика будет установлен на рабочем месте и подключен к серверу.

Проверить, успешно ли выполнена установка агента загрузчика, можно с консоли, где в дереве пользователей должна появиться пиктограмма  с именем конечной рабочей станции. Клиент может быть удаленно установлен на конечной рабочей станции, на которой уже установлен агент загрузчика.

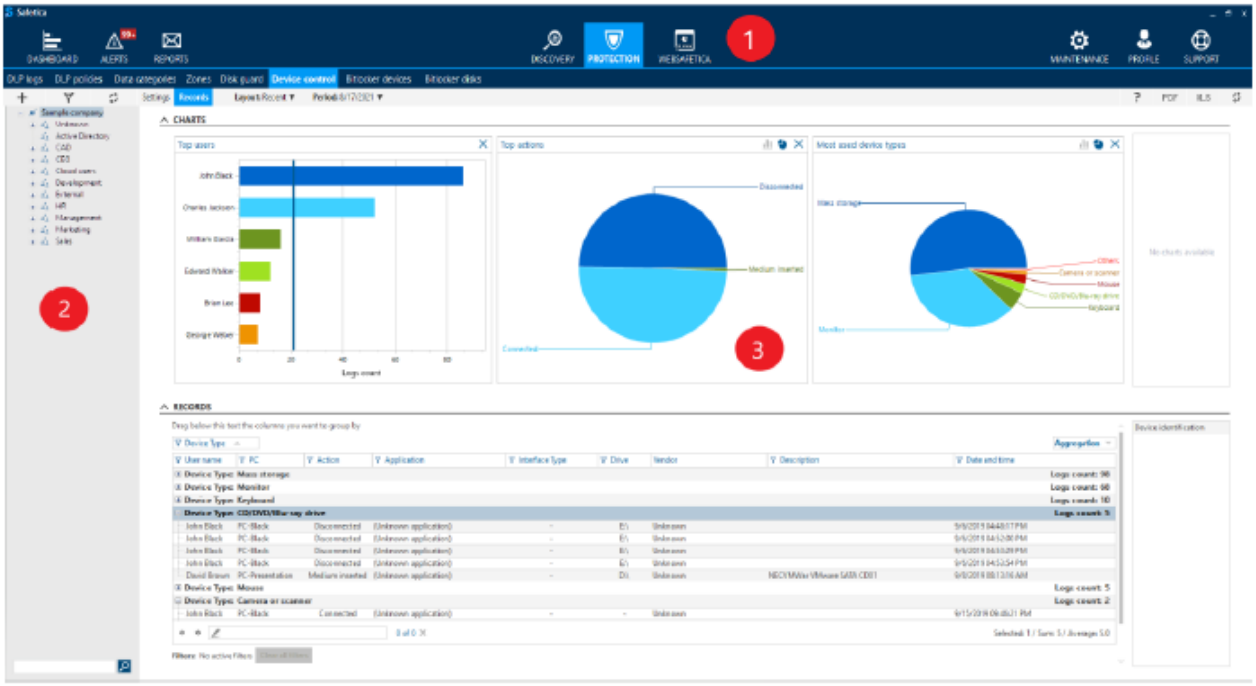
Примечание. Компонент агента загрузчика будет автоматически установлен вместе с клиентом.

4. Консоль

Все функции и компоненты Safetica (клиенты, серверы и базы данных) управляются через веб-консоль или консоль, установленную на компьютере. Также она позволяет отображать выходные данные мониторинга, статистику и диаграммы. После запуска консоли вы должны выполнить вход с помощью учетной записи пользователя. Отображаемые элементы и набор функций Safetica зависят от прав пользователя, выполнившего вход в систему. Вы можете управлять пользователями и правами через меню Управление доступом.

4.1. Описание интерфейса

После запуска консоли Safetica вы увидите следующий интерфейс.



Главное меню (1)

Переключатель режима консоли расположен в нижнем левом углу главного меню.

- *Режим настроек.* В этом режиме отображаются настройки модулей Safetica (кроме модуля Discovery). Настройки всех функций модуля Discovery можно найти здесь: *Discovery -> Настройки функций*. Этот режим не связан с настройками консоли или сервера. Они управляются с помощью отдельных настроек в разделе Обслуживание. Функции, настроенные для групп, пользователей или компьютеров, указаны в дереве пользователей. Изменения в настройках действуют только если они сохранены с помощью кнопки  в правом верхнем углу окна настроек функций. Изменения можно отменить с помощью кнопки  .
- *Режим визуализации.* В этом режиме записанные данные, итоговые отчеты, диаграммы и статистика отображаются в разделе функций Safetica. Данные о группах, пользователях и компьютерах, идентифицированных в дереве пользователей, отображаются за определенный период времени.

Слева есть пиктограммы, которые можно использовать для формирования различных представлений итоговой информации.

- *Dashboard* — обзор данных, собранных по всем активным функциям.
- *Предупреждения* — настройки автоматического предупреждения.
- *Отчеты* — настройки отправки регулярных отчетов.

В центре находятся пиктограммы, используемые для переключения между тремя основными модулями

Safetica:

- Discovery
- Protection
- Websafetica

Справа находятся пиктограммы, которые используются для администрирования всех компонентов Safetica, а также для перехода к справочной информации.

- *Обслуживание* — управление и конфигурирование подключенных серверов и клиентов, а также агента загрузчика.
- *Профиль* — базовые настройки вашей учетной записи, такие как подключение к серверу и пользовательские настройки консоли.
- *Помощь* — доступ к справке Safetica.

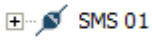
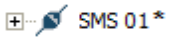
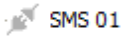
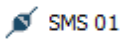
Под верхней панелью с элементами управления консолью расположен список функций модулей. Этот список изменяется в зависимости от используемого в данный момент модуля — Discovery, Protection или Настройки (Maintenance).

Дерево пользователей (2)

Дерево пользователей находится на консоли с левой стороны, под верхней панелью инструментов. Все серверы Safetica, к которым вы подключены, отображаются в этом дереве. Новое подключение к серверу можно настроить в разделе *Профиль*. Каждый сервер в дереве имеет группы, пользователей и компьютеры, подключаемые к нему. В зоне отображения или просмотра (раздел 3 на рисунке) отображаются настройки или данные, вычисленные для выбранных элементов дерева с помощью соответствующих функций. Несколько элементов можно выбрать, удерживая кнопки *Ctrl* или *Shift* и одновременно отмечая нужные элементы. Дополнительную информацию о сервере можно прочитать в разделе Архитектура.

Элементы дерева

Корневые элементы дерева — серверы, к которым вы подключены через консоль. Следующие пиктограммы в дереве пользователей обозначают статус подключения каждого пользователя:

-  — вы подключены через консоль к серверу с именем SMS 01.
-  — (где за именем сервера следует символ звездочки) — дерево изменилось и его нужно обновить. Это можно сделать, например, с помощью кнопки  .
-  — ваша консоль не подключена к серверу, так как сервер недоступен или выключен.
-  — в некоторых режимах просмотра этот параметр общий для всего сервера. В этом случае отображаются только те серверы в дереве пользователей, к которым вы подключены через консоль (дерево нельзя распаковать).

Дополнительную информацию об использовании дерева пользователей вы можете найти в разделе «Справка» в теме о функциях, настройках, и визуализации собранных данных.

Основные элементы дерева:

- — пользователь, выполнивший вход в компьютер с помощью клиента или агента загрузчика и в данный момент находящийся в сети. Если пользователь уходит из сети, его пиктограмма становится серой:
- — компьютер, на котором установлен клиент и который сейчас находится в сети. Если компьютер отключается от сети, его пиктограмма становится серой: . Если на компьютере установлен агент загрузчика, вы можете перезапустить клиентскую службу *Перезапуск службы* или весь компьютер *Перезагрузить компьютер* из контекстного меню.
- — компьютер, на котором установлен агент загрузчика и который сейчас находится в сети. Через контекстное меню вы можете перезапустить клиентскую службу *Safetica Client Service* на компьютере или перезагрузить весь компьютер.
- —группа, в которую входят пользователи, компьютеры или другие группы.

Дальнейшие операции с деревом пользователей, такие как добавление групп, удаление, переименование пользователей и компьютеров, выполняются с использованием контекстного меню, которое вызывается щелчком правой кнопки мыши по элементу дерева. Элементы дерева можно переместить с помощью мыши (перетаскиванием). Контекстное меню для компьютеров дополнено следующими параметрами:

- *Переадресация.* Перенаправляет клиента на другой сервер. См. раздел Переадресация клиента на другой сервер.
  - — переадресация настроена.
  - — переадресация завершена.
- *Разрешение неизвестного сертификата.* Эта функция разрешает клиенту подключиться к другому серверу (и получить сертификат с другого сервера).
- *Включить активное управление* — в этом режиме перенос настроек в клиент и их сохранение в базе данных займут минимальное время. Управление клиентами в течение указанного периода будет выполняться практически мгновенно. Активное управление имеет более высокий приоритет, чем интервал настройки и переноса записей, настроенный в разделе *Настройки клиента*, но его можно включить лишь на ограниченный период (1, 2, 4 или 24 часа). Если на компьютере включено активное управление, пиктограмма в дереве изменится на следующую:
  - — настроено активное управление, но клиент еще не обновил настройки;
  - — настроено и работает активное управление.

Другие свойства дерева пользователей:

- Группы могут быть вложенными, то есть одна группа может иметь несколько подгрупп. Однако у каждой группы может быть только одна родительская группа. Группы отмечены пиктограммой .
- Группы могут содержать пользователей и компьютеры.
- Пользователи и компьютеры могут быть помещены в несколько групп (один и тот же пользователь или компьютер может быть представлен в нескольких разных группах или ветках одновременно).

Встроенные группы

В дереве пользователей существуют две встроенных группы:

- *Неизвестные* — эту группу нельзя удалить. После подключения нового клиента вновь подключенные пользователи и компьютеры помещаются в эту группу. Вы можете копировать и вставлять/перемещать этих пользователей и компьютеры из группы *Неизвестные* в группы, которые создали сами. Если вы удалите пользователя или компьютер из всех своих групп, они вернутся обратно в группу *Неизвестные*. То же правило применяется к пользователям и компьютерам из группы, которая была удалена из дерева пользователей. Окончательно удалить пользователей или компьютеры можно, удалив их из группы *Неизвестные.*
- *Active Directory* — этот элемент нельзя удалить. Он используется для синхронизации сервера с Active Directory. Вы можете выбрать дерево Active Directory в разделе Настройки сервера. После подтверждения операции все пользователи и компьютеры будут скопированы в группу AD. Эта группа доступна только для чтения, а значит вы не можете создавать в ней новых пользователей и компьютеры или удалять их, но зато можете скопировать их в другие группы, доступные для настройки. Группа AD используется только для организации связи между деревом Active Directory и деревом пользователей в консоли.

Элементы управления деревом

Есть несколько элементов управления деревом пользователей:

- Кнопка  раскрывает все узлы в дереве пользователей.
- Кнопка сворачивает все узлы в дереве пользователей.
- Кнопка  отображает экспресс-фильтр для дерева. Фильтр можно использовать для выбора элементов, которые будут отображаться в дереве. Щелкните по нужному фильтру, чтобы его включить. Щелкните еще раз, чтобы отключить выбранный фильтр. Вы можете настроить одновременно несколько фильтров. В этом случае в дереве будут отображаться только те элементы, которые соответствуют всем вашим фильтрам. Для выбора фильтров необходимо нажать кнопку ОК.
- Кнопка  обновляет дерево пользователей.

Зона отображения/просмотра (3)

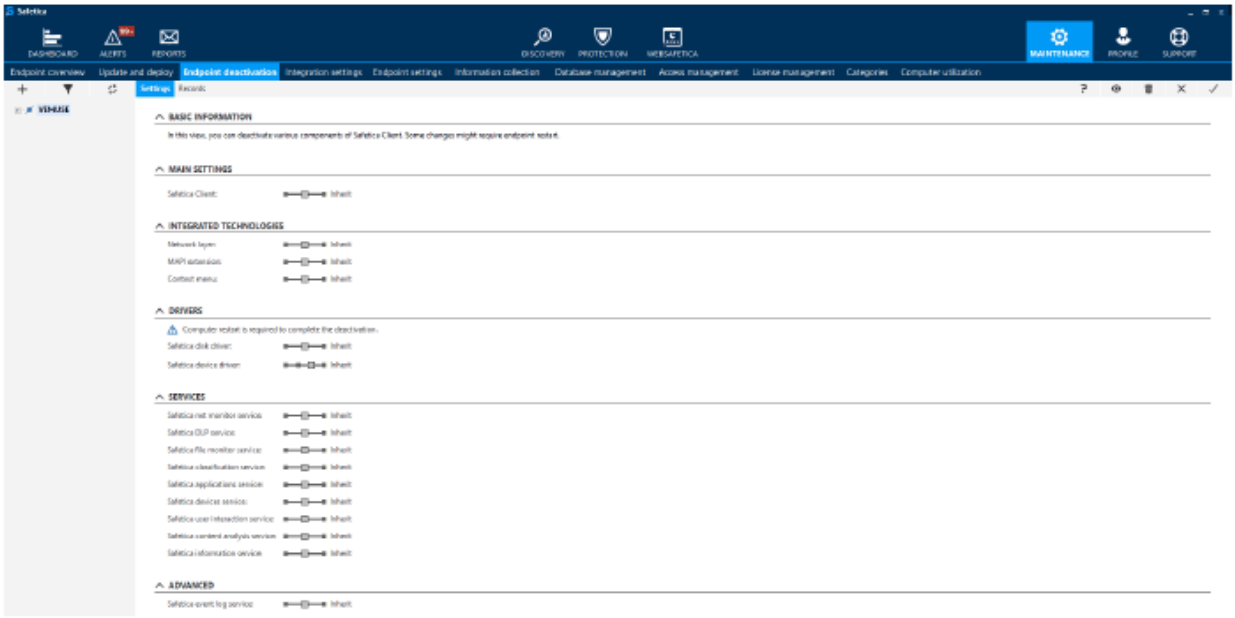
Зона отображения, также называемая зоной просмотра, используется для визуализации данных и изменения настроек отдельных функций. Содержимое зоны просмотра изменяется в зависимости от того, какую функцию вы в данный момент просматриваете, и от текущего режима (настройки, визуализация и т. п.). При описании отдельных функций мы будем называть эту зону зоной просмотра.

Для переключения между функциями модуля выберите модуль в главном меню, чтобы отобразить список его функций, а затем переместите функцию в область просмотра, щелкнув по ее названию.

4.2. Режим настроек

В режиме настрое вы можете конфигурировать функции Safetica для пользователей, групп или компьютеров. На первом шаге всегда выбирайте реленвантных пользователей, группы или компьютеры в дереве пользователей.

Вы можете войти в режим настроек, нажав на кнопку *Настройки* в верхнем сером баннере.



Просмотреть раздел справки по какой-либо функции можно с помощью кнопки ?.

Настройки, выполняемые через дерево пользователей, имеют следующие свойства:

Режим настроек

Вы можете установить следующие режимы почти для каждой функции:

- *Отключено* — функция не активирована.
- *Наследование* — режим функции наследуется. Настройка наследуется от родительской группы, если она задана в одной или нескольких родительских группах.
- *Включено* — соответствующая функция активирована.

Выбранная настройка присваивается только пользователям, группам или компьютерам, выделенным в дереве пользователей. Чтобы применить настройки, вам нужно сохранить изменения, нажав на ✓.

Отменить изменения вы можете, нажав на ✕ в правом верхнем углу.

Элементы дерева пользователей, для которых настроена функция (*вкл., выкл.*), подсвечиваются в дереве синим цветом.

Наследование настроек

- Вы можете создавать настройки для пользователей, групп (включая ветки) и компьютеров с помощью дерева пользователей на консоли.
- Настройка группы наследуется ее подгруппами, пользователями и компьютерами. Настройка, сделанная для группы, также применяется ко всем подгруппам, пользователям и компьютерам в этой группе.
- Настройка на более низком уровне дерева пользователей считается более строгой, а значит имеет более высокий приоритет. К примеру, вы создаете настройки для группы, а затем — для пользователей или компьютеров в этой группе. Более приоритетной будет настройка, сделанная для пользователей или компьютеров.

Коротко:

- *Явная настройка* — настройка, выбранная вручную для конкретных пользователей, групп, компьютеров или всей ветки. Вы можете удалить явную настройку в функции, нажав на кнопку  .

- *Эффективная настройка* () — настройка, вычисленная автоматически путем объединения настроек для отдельных объектов. Вычисление выполняется путем объединения настроек в порядке прохода по дереву пользователей от объекта на самом низком уровне (с высоким приоритетом) до корня или ветки (с более низким приоритетом), а также путем присоединения индивидуальных настроек.

Расчет эффективности настройки

В консоли всегда отображается явная настройка. С помощью кнопки  можно перейти к отображению эффективной настройки для текущей функции и выделенных элементов в дереве пользователей.

Как было описано выше, расчет выполняется в направлении от листьев (например, пользователя или компьютера) в дереве пользователей к корню. Настройка, сохраненная для пользователя, имеет более высокий приоритет, чем настройки группы, к которой относится этот пользователь. Объединение выполняется следующим образом. Если для пользователя ничего не установлено, используется настройка его группы. Если установлены настройка для группы и настройка для пользователя, будет действовать настройка для пользователя. Это относится также к вложенным компьютерам и группам.

Компьютер или пользователь, находящиеся в нескольких группах

Вы можете заносить компьютеры или пользователей в несколько групп одновременно. Если пользователь или компьютер находятся в нескольких группах, для расчета эффективных настроек будут выполнены следующие шаги:

1. Эффективные настройки рассчитываются для каждого пути, который существует для этого пользователя или компьютера, что дает нам две (или более) эффективных настройки.
2. Из этих настроек выбирается одна, наиболее «строгая». Например:

- Настройки *Включено* и *Выключено* объединяются в настройку *Включено*. Пример: включение мониторинга приложений.
- Значения интервала всегда объединяются в более строгий интервал.
- Для некоторых функций, например, для Контроля приложений или Веб-контроля, создан список правил и можно указать тип правил: список разрешений или список запретов. Если настройки отличаются, применяется список разрешений.
- Если типы списков (*список разрешений* или *список запретов*) одинаковы, эти списки объединяются в один. Объединяются только списки одинаковых типов (*список запретов* или *список разрешений*).

Настройки для пользователя и компьютера

Дерево пользователей позволяет создавать настройки для пользователей и компьютеров. Настройки компьютера применяются к каждому пользователю, который зашел в систему с этого компьютера, следующим образом:

1. Итоговые настройки для пользователя на конкретном компьютере вычисляются путем объединения *эффективных настроек* для этого пользователя и этого компьютера.

2. Результат объединения настроек для компьютера и для пользователя считается окончательным и применимым. Объединение выполняется следующим образом.

- Если настройка не указана для пользователя, применяется настроенное для компьютера значение.
- Если ни для пользователя, ни для компьютера ничего не установлено, будет использоваться настройка по умолчанию. Настройки по умолчанию описаны в разделе, посвященном отдельным функциям.
- Все настройки, установленные для обоих объектов, применяются с учетом приоритетов, которые можно настроить для каждого модуля в разделе Настройки клиента. По умолчанию (если приоритеты не настроены), компьютер имеет более высокий приоритет (его настройки применяются вместо настроек пользователя).
- Списки правил объединяются, если для них выбраны одинаковые режимы. В противном случае выбирается один из списков, также с учетом приоритетов.

Общая политика использования настроек

Safetica предоставляет широкий ряд настроек, позволяющих тщательно отладить функции безопасности в ваших ветках. Однако неаккуратный выбор настроек может привести к ухудшению работы всей системы. По этой причине мы рекомендуем использовать сложные настройки только при наличии достаточного опыта.

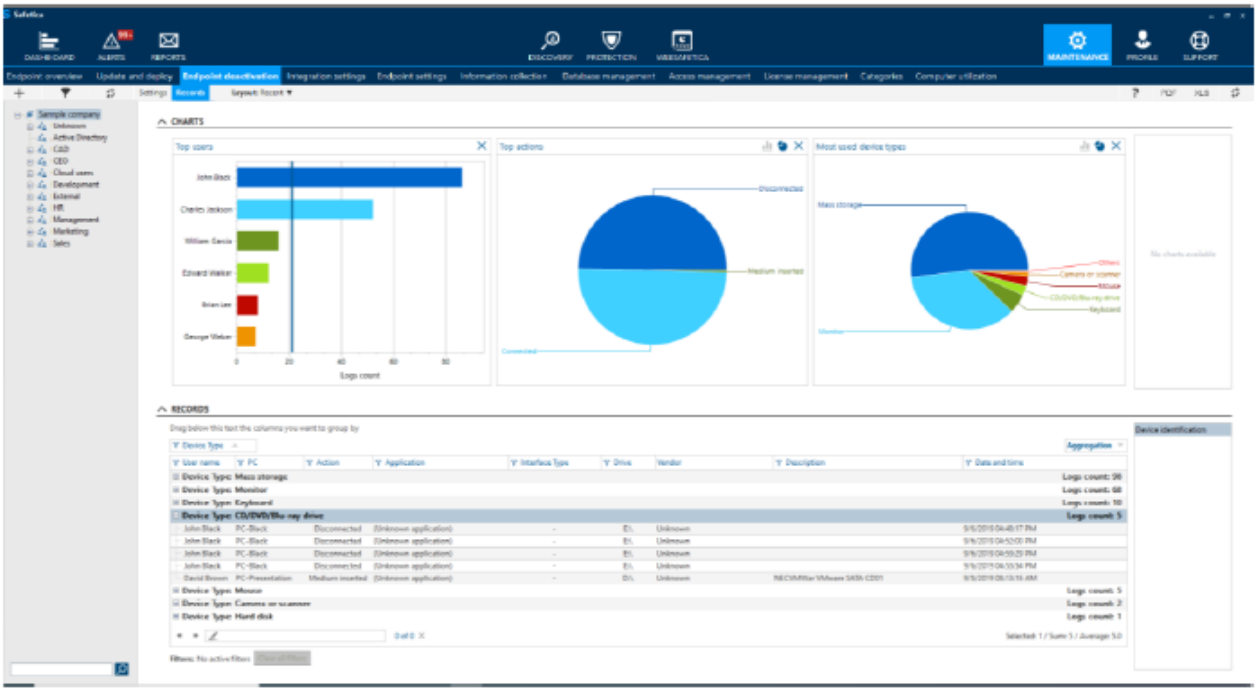
Если вы согласны использовать простые варианты обобщенных настроек, вот несколько рекомендаций общего характера.

- Устанавливайте настройки только для групп, а не для пользователей или компьютеров. После этого объединяйте в эти группы конкретных пользователей и компьютеры в зависимости от того, какие настройки вы хотите для них применить.

  Пример. Предположим, что в вашей компании три отдела: маркетинговый отдел, отдел разработок и отдел технической поддержки. Вы хотите, чтобы для сотрудников разных отделов использовались разные модули и функции. Не присваивайте настроек сотрудникам этих отделов, просто выбирая каждого пользователя в дереве. Вместо этого создайте группу для каждого из отделов и распределите сотрудников по этим группам. Затем создайте настройки для каждой группы. Таким образом настройки будут установлены для сотрудников в этих группах.
- Если возникла необходимость настроить что-то для конкретного пользователя, его следует рассматривать отдельно и не нужно включать в эту группу. Лучше всего для таких пользователей создавать отдельную группу или подгруппу, чтобы не применять никакие настройки на уровне индивидуального пользователя. Вполне вероятно, что позднее вы захотите применить такие же настройки и для другого пользователя. В этом варианте вы сможете просто включить в нужную группу нового пользователя.
- Продуманное распределение по группам позволяет избежать путаницы, если возникнет необходимость перенести пользователя в другую группу. Вы будете ожидать, что пользователь унаследует все настройки от новой группы, но, если вы ранее установили для него индивидуальные настройки, они будут иметь более высокий приоритет.
- Кроме того, настройки на уровне групп требуют меньше места для хранения в базе данных, чем настройки для отдельных пользователей.

4.3. Режим визуализации

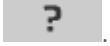
Чтобы перейти в режим визуализации, нажимте кнопку Records в верхнем сером баннере. В зависимости от конкретного модуля и функции, из которых вы перейдете в этот режим, вам будут предложены разные данные и диаграммы по тем элементам, которые вы выбрали в дереве пользователей. Некоторые функции не могут быть визуализированы.



Вы увидите записи и диаграммы с данными о тех пользователях, компьютерах и/или группах, которые выделены в дереве пользователей. Также вы можете выбрать конкретный период для просмотра собранных данных мониторинга. Для этого нажмите на кнопку *Период* в верхней левой части экрана. У вас есть несколько вариантов указания периода:

- *Сегодня* — отображаются записи за текущий день.
- *Вчера* — отображаются записи за предыдущий день.
- *На прошлой неделе* — отображаются записи за семь последних дней, включая текущий.
- *Прошлый месяц* — отображаются записи за 31 последний день, включая текущий.
- *Один день* — вы можете просмотреть записи за один выбранный день. Вы можете выбрать целый день или временной интервал. Подтвердите свой выбор кнопкой *Подтвердить дату.*
- *Диапазон* — вы можете просмотреть записи за определенный период времени. Вы можете выбрать первый и последний день диапазона. Также вы можете указать время. Подтвердите свой выбор кнопкой *Подтвердить дату.*

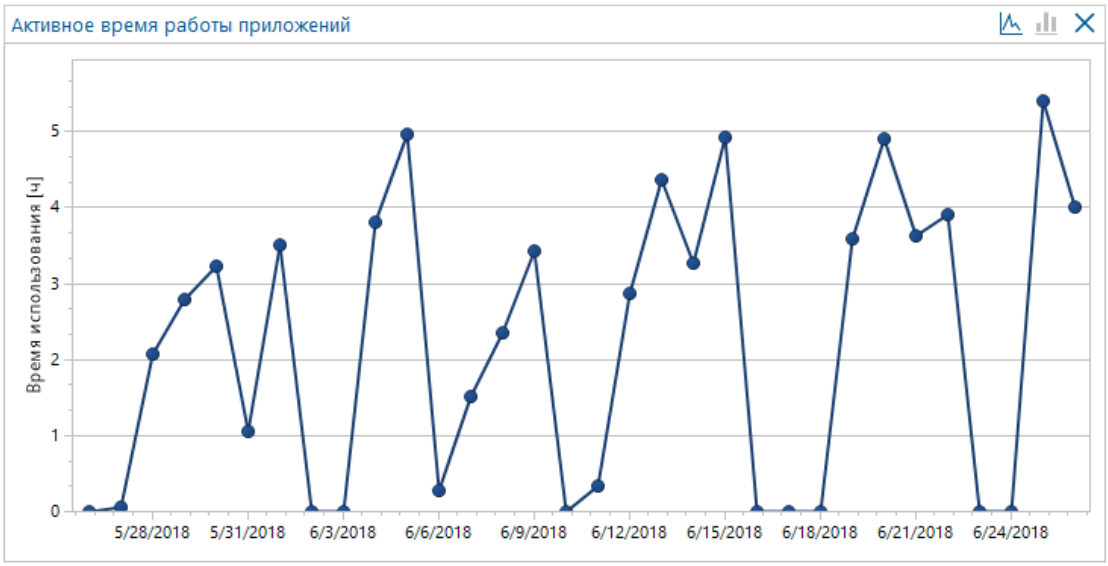
Вы можете перезагрузить записи и диаграммы, нажав на кнопку  в верхнем правом углу.

Просмотреть раздел помощи по какой-либо функции можно с помощью кнопки  .

Диаграммы

В верхней части экрана в режиме визуализации расположена зона для отображения диаграмм. Список диаграмм, доступных для просмотра, находится в правой части экрана.

- Чтобы увидеть диаграмму, вам достаточно перетащить ее с панели в правой части в зону оповещений, где можно разместить одновременно несколько диаграмм.
- Чтобы удалить диаграмму из области просмотра, нажмите на кнопку . Тем самым вы переместите диаграмму обратно в список с правой стороны.
- Нажимая на кнопки , и , вы можете изменять тип диаграммы (круговая, столбчатая или линейная).
- Щелкнув по отдельному сектору или столбцу, вы установите автоматический фильтр для соответствующей колонки, который будет сразу применен ко всем расположенным ниже записям. Вы можете применять фильтры одновременно по нескольким секторам и/или столбцам на диаграммах в зоне отображения. Чтобы удалить фильтр, просто щелкните по кругу сектору или столбцу еще раз.
- На некоторых линейных диаграммах можно выбирать временной диапазон с помощью мыши. Для отмены выбора нажмите на кнопку .



- На некоторых диаграммах отображается синяя вертикальная линия, которая показывает среднее значение данных в этой диаграмме.

Записи

В нижней части экрана в режиме визуализации отображается таблица подробных записей. Список столбцов, доступных в текущем режиме просмотра, находится в правой части экрана.

- Для отображения столбца в таблице нужно перетащить этот столбец в зону таблицы.
- Щелчок по кнопке в заголовке столбца отобразит фильтр для этого столбца. Заполните и подтвердите фильтр, нажав на кнопку *OK*, чтобы применить этот фильтр к столбцу.
- Под таблицей вы увидите поле поиска. При вводе текста будут выделяться слова, по которым выполняется поиск в таблице. Щелкните по , чтобы убрать выделение.
- Перетащите заголовок столбца в зону над таблицей, чтобы сгруппировать данные таблицы по этому столбцу. Вы можете перетащить несколько столбцов в зону над таблицей.

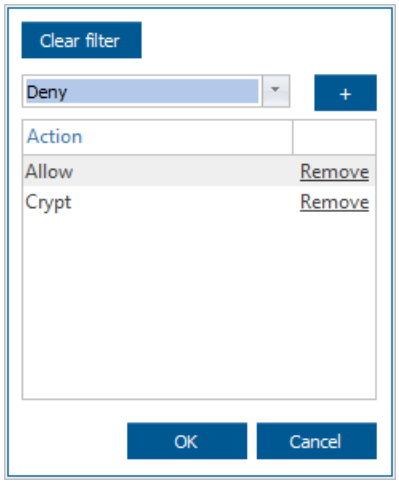
Фильтры

Вы можете фильтровать записи. Открыть фильтр для любого столбца можно щелчком на кнопке в заголовке соответствующего столбца. В верхней части диалогового окна введите текст или выберите элемент из списка, чтобы выбрать условие для фильтрации столбца. Щелчок по кнопке + добавит этот элемент в список условий фильтра (также вы можете добавить элементы, подтвердив их кнопкой *OK*). В списке может быть несколько условий. После подтверждения фильтра кнопкой *OK* таблица будет показывать только те записи, которые соответствуют условиям фильтра.

Фильтр для столбца не установлен

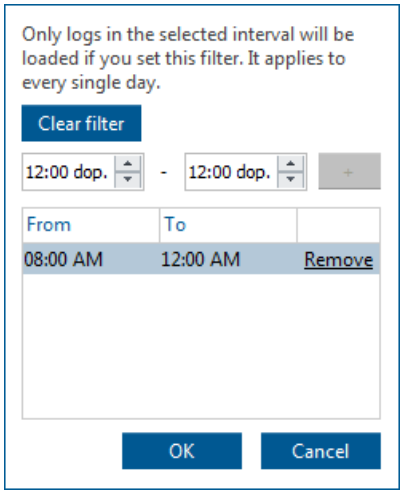
Для столбца установлен фильтр. Заголовок можно выделить жирным шрифтом

Вы можете установить фильтр, щелкнув по сектору или столбцу диаграммы, как описано выше в разделе о диаграммах. Вы можете удалить все установленные фильтры, нажав на кнопку *Сбросить фильтр.*

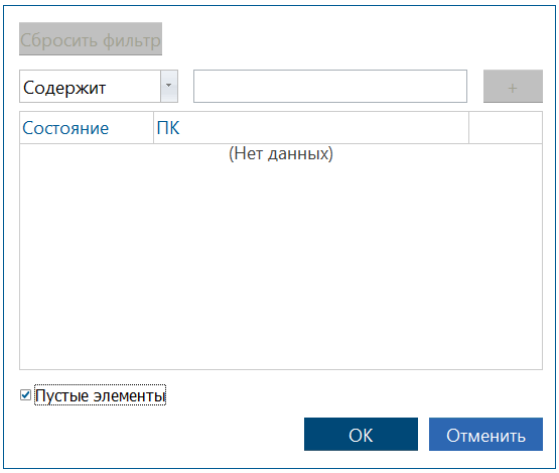


Можно настроить фильтр для любого столбца *Дата и время* и ввести временной интервал, чтобы указать, с какого момента отображать записи этого дня.

Вы также можете ввести несколько интервалов одновременно.



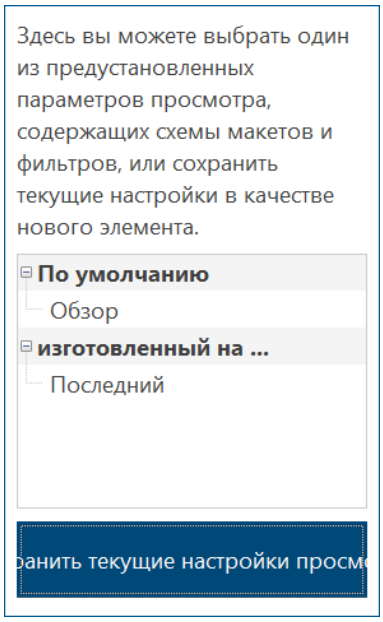
В текстовых фильтрах можно выполнять поиск пустых элементов. Для этого нужно установить флажок напротив пункта *Пустые элементы* в соответствующем фильтре.



Форматы

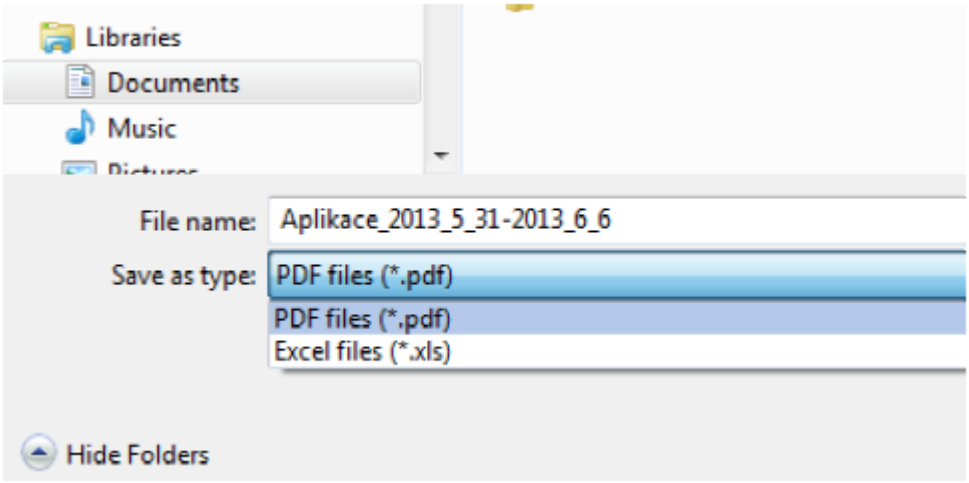
Можно создать собственный формат диаграмм, столбцов и фильтров для каждой функции. Для этого используется менеджер форматов. Чтобы открыть менеджер форматов, нажмите на нужный формат рядом с заголовком *Раскладка* в левом верхнем углу.

- Каждый пользователь Safetica может создать собственный формат визуализации для каждой функции.
- Также вы можете настроить формат визуализации *по умолчанию*, нажав на элемент.
- По умолчанию в менеджере форматов. Элемент *Последний* позволяет выбрать последний использованный формат.
- Чтобы сохранить текущий формат диаграмм, столбцов и фильтров, щелкните *Сохранить текущие настройки отображения*.



Экспорт в PDF и XLS

Можно экспортировать отображаемые диаграммы в формате PDF или Excel с помощью кнопки PDF или XLS в правом верхнем углу.



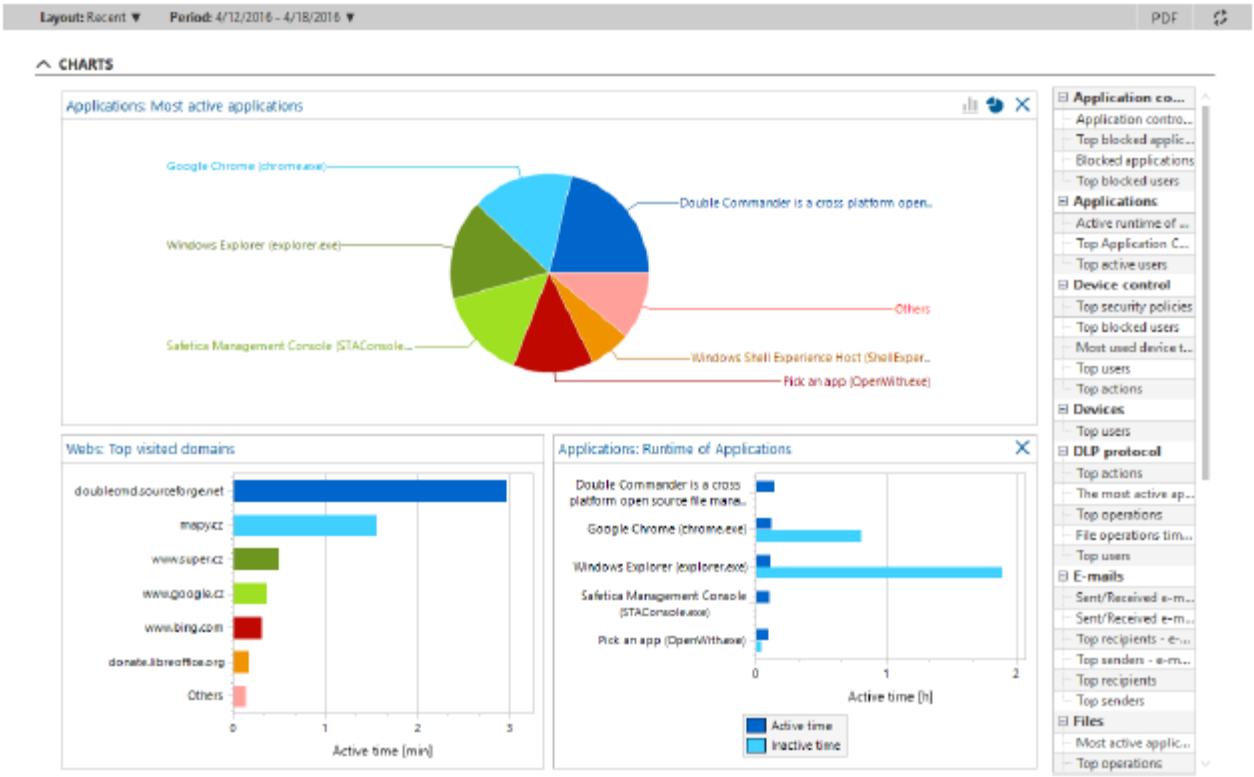
Примечание. Все данные по выбранным пользователям, временному периоду в визуализации и настройкам фильтра будут экспортированы в Excel. Группы записей также экспортируются в Excel.

4.4. Управление и настройки

4.4.1. Dashboard

В режиме просмотра панели управления вы можете отобразить в одном месте диаграммы из любых модулей и функций. Это позволяет объединить наиболее важные данные, чтобы получить представление о состоянии вашей организации. Это могут быть результаты мониторинга, список инцидентов, связанных с нарушением безопасности, либо журналы заблокированных страниц или приложений.

Отчеты можно просмотреть, нажав на кнопку *Dashboard* в верхнем левом углу консоли Safetica. Отчеты будут отображаться только для пользователей, групп, компьютеров или серверов, выбранных в древе пользователей.



Данные панели управления показываются только для пользователей, компьютеров или групп, выбранных в дереве пользователей. Список доступных диаграмм расположен справа. Диаграммы по отдельным функциям распределены по функциям и модулям. Отобразить их можно, нажав на них и перетащив в зону просмотра диаграммы. Чтобы удалить группу диаграмм из списка, нажмите на кнопку ✕ в правом верхнем углу группы диаграмм. Больше информации об использовании графиков можно найти в разделе о журналах и режиме визуализации.

Отображаемые диаграммы можно экспортировать в формате PDF с помощью кнопки PDF.

4.4.2. Предупреждения

Предупреждения оповещают событиях в системе Safetica. Предупреждения используются большинством компонентов Safetica. Администратор безопасности или любой другой авторизованный администратор может настроить оповещения о выбранных чрезвычайных ситуациях. Если произойдет любое из таких событий, администратор получит сообщение через консоль Safetica или по электронной почте в зависимости от настроек.

Предупреждения можно просмотреть, нажав на кнопку *Предупреждения* в верхнем левом углу консоли.

Настройки

Предупреждения настраиваются для сервера, выбранного в дереве пользователей. Чтобы применить эти настройки, нужно сохранить изменения с помощью кнопки ✓. Также вы можете отменить изменения кнопкой ✕ справа вверху.

Слева на экране вы найдете список созданных наборов предупреждений. Когда вы выберете набор

предупреждений из этого списка, справа появится информация о предупреждениях: имя, список оповещений, список пользователей, к которым относится предупреждение, а также список рассылки предупреждений.

В столбце *Владелец* вы найдете имя учетной записи для подключения к серверу, под которой было создано предупреждение.

Нажмите на кнопку *Изменить,* чтобы обновить соответствующий элемент.

Щелкните по кнопке *Удалить*, чтобы удалить предупреждение.

В настройках вы можете выбрать собственные наборы предупреждений. Для каждого набора можно выбрать разные предупреждения и указать целевые группы, пользователей или компьютеры, а также способ доставки предупреждения — консоль, электронная почта или оба этих средства.

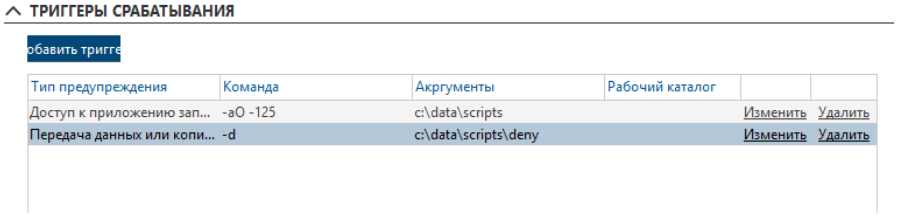
Предупреждения подразделяются на четыре основных категории:

- *Предупреждения безопасности.* Эти предупреждения направляются сразу после возникновения соответствующей ситуации, связанной с безопасностью. Для некоторых предупреждений вы можете указать, к каким категориям данных или типам оборудования будет применяться это предупреждение. Если не указано предпочтений относительно категории или устройства, предупреждение будет применяться ко всем. После выбора пунктов *Все Любая категория данных* или *Все устройства* откроется диалог, где вы можете указать категории данных или устройства, к которым будут применяться предупреждения.
- *Информационные предупреждения.* Эти предупреждения отправляются ежедневно и еженедельно при превышении определенного значения за день или неделю. Для некоторых предупреждений можно указать категорию веб-сайтов или приложений, к которой будут применены введенные значения за день или неделю. Если не указано категорий, значение будет применяться ко всем. Категории можно выбрать в диалоговом окне. Чтобы отобразить категории для соответствующего предупреждения, выберите пункт *Добавить категорию.* Таким образом можно добавить несколько категорий. Для каждой категории можно настроить разные дневные или недельные значения.
- *Служебные предупреждения.* Используются для оповещения администратора об инцидентах, связанных с безопасностью.
- *Умные предупреждения.* Это предупреждения об инцидентах, связанных с безопасностью, которые отображаются только в WebSafetica. Они не будут отображаться на консоли и не будут отправляться по электронной почте.

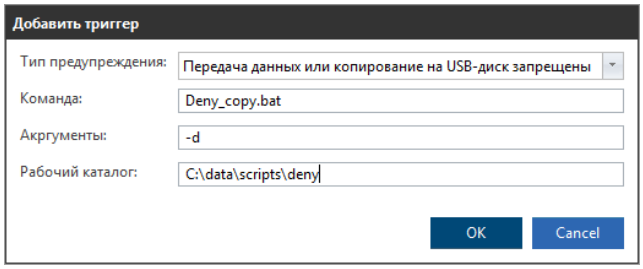
После установки автоматически создается предупреждение по умолчанию, которое содержит все предупреждения из категории *Сервисные предупреждения -> Сервис.*

Триггеры срабатывания

В разделе триггеров действий можно настроить команду или сценарий, которые будут запускаться с конкретными параметрами в выбранной папке с учетом данных об активности. Команда будет выполняться на клиентской станции под учетной записью пользователя, ставшего причиной инцидента. Эти настройки применяются ко всему серверу.



Вы можете отобразить диалог для добавления нового триггера действия, нажав на кнопку *Добавить триггер*.



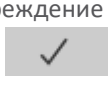
Настройка нового предупреждения

1. Для создания нового набора предупреждений нажмите *Новое правило.*
2. Введите название и описание предупреждения, затем нажмите *Далее* справа внизу.
3. Вы увидите списки разных типов предупреждений, отсортированных по категориям. Выберите нужное предупреждение из списка. Вы можете выбрать несколько типов предупреждений из нескольких категорий. После завершения выбора нажмите *Далее.*

   Примечание. Информационные предупреждения отправляются только на основании поведения пользователя. Для получения информационных предупреждений пользователи должны быть включены в набор предупреждений. Предупреждения о безопасности создаются для пользователей и/или компьютеров. Они отправляются с рабочей станции сразу же после инцидента.
4. На следующем шаге нажмите *Добавить пользователя*. Появится диалог, в котором вы сможете выбрать компьютеры, группы или отдельных пользователей. Предупреждения, которые вы выбрали на предыдущем шаге, будут отправляться только тем пользователям, компьютерам или группам, которые вы выберете на этом шаге. Нажмите Далее.
5. На этом шаге нужно выбрать адреса электронной почты, на которые будут отправляться предупреждения. Для этого нажмите *Добавить email.* Также вы можете получать предупреждения напрямую в консоль. Для этого воспользуйтесь ползунком *Отправить в консоль* . Вы можете включить регистрацию данных в системных журналах серверов *SIEM / Syslog*. Просто введите адрес сервера и порт. Сервер должен быть доступен с соответствующего сервера.

   После завершения нажмите *Далее.*

   Примечание 1. Сервер SMTP должен быть настроен на отправку почты. Это можно сделать, последовательно открыв Профиль -> Настройки -> Исходящий (SMTP) сервер.

   Примечание 2. Новое оповещение, поступающее через консоль, отображается в виде номера над пиктограммой предупреждений в правом верхнем углу консоли. Этот номер обозначает количество предупреждений, назначенных для отправки в консоль, но еще не прочитанных.
6. На последнем этапе отображается обзор настроек, которые вы создали при настройке предупреждения. Чтобы добавить предупреждение к списку, щелкните по кнопке *Конец.* Для сохранения изменений нажмите на кнопку  в правой верхней части.

Визуализация

Все предупреждения записываются. Их можно просмотреть позднее в режиме визуализации. Пользователь Safetica видит только предупреждения, созданные под его учетной записью, как показано здесь.

В верхней части вы найдете статистику и диаграммы. В нижней части вашего экрана есть список сгенерированных предупреждений. Щелчок на нужной статистике в нижней части экрана отображает предупреждения, относящиеся к этой статистике. Непросмотренные предупреждения выделяются.

Предупреждения, которые настроены для отправки в консоль, включаются в общее число новых предупреждений, отправленных в консоль. Это значение отображается над *значком предупреждений* в верхнем левом углу консоли.

4.4.3. Отчеты

Включенные в Safetica средства автоматической отчетности позволяют получать регулярные сведения о текущей ситуации в вашей организации. Вы можете создать свой собственный формат отчетов. Для каждого отчета можно выбрать его содержание, а также каких пользователей, групп или компьютеров он будет касаться, кто должен его получать. Чтобы изменить настройки для отчетов войдите в главное меню *Отчеты.*

Настройки

Отчеты настраиваются для сервера, выбранного в дереве пользователей. Для применения этих настроек нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  вверху справа.

В левой части зоны просмотра отображается список зарегистрированных записей. После выбора отчета в левом списке с правой стороны появится следующая информация: название, дата последнего создания, список включенных отчетов, список пользователей, к которым относится отчет, а также список адресов электронной почты, на которые он будет отправлен, и формат отправки.

Нажмите *Создать сейчас,* чтобы немедленно создать отчет.

В столбце *Сделано* вы найдете имя учетной записи для подключения к серверу, под которой был создан отчет.

Нажмите на кнопку *Изменить* рядом с соответствующим элементом отчета, чтобы обновить его. Нажмите на кнопку *Удалить,* чтобы удалить отчет.
Примечание. Вы также можете создавать отчеты в WebSafetica.

Создание нового отчета

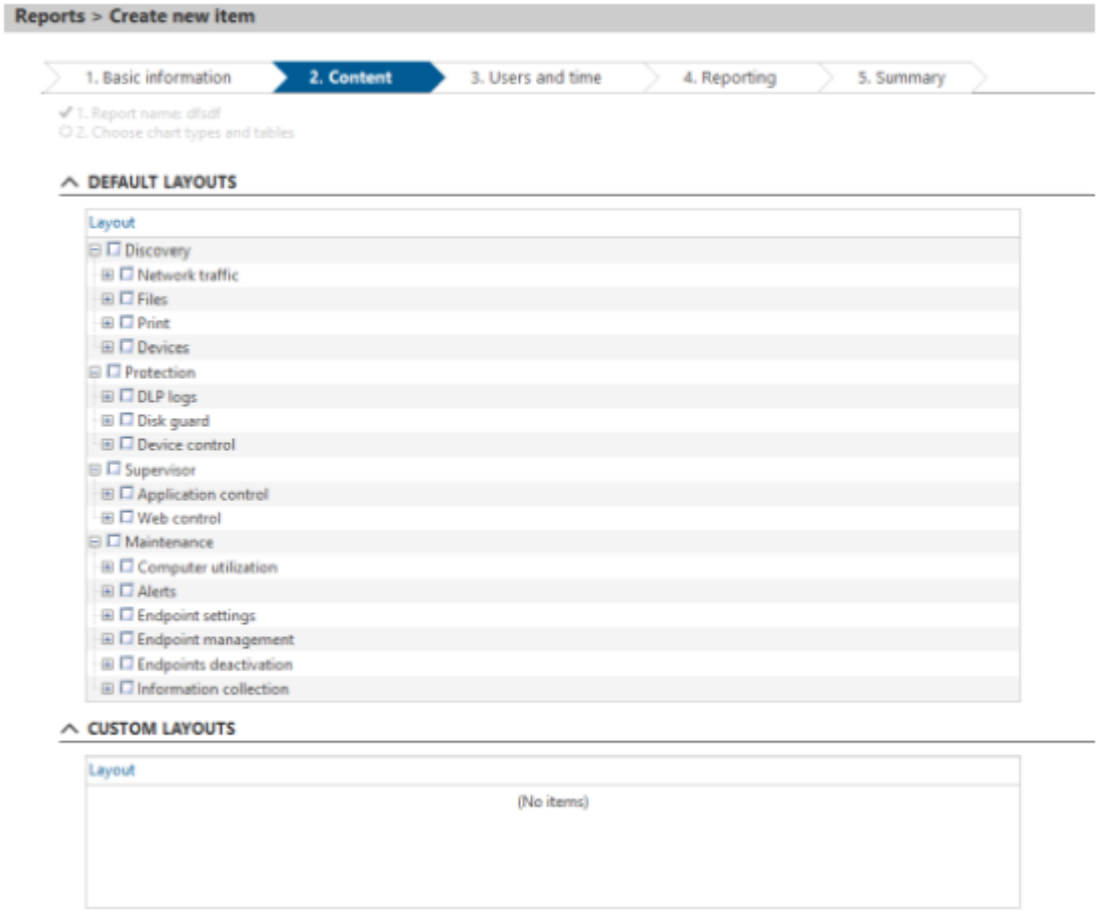
1. Для создания нового отчета нажмите *Новое правило.*
2. Введите название и описание нового отчета, затем нажмите *Далее* справа внизу.
3. Здесь находится список доступных отчетов. Этот список основан на режиме просмотра отчетов (см. *Режим визуализации -> Макеты*), где вы можете создать пользовательский формат диаграмм, столбцов и фильтров для режимов визуализации каждой функции Safetica.

- *По умолчанию* — здесь собраны стандартные отчеты с диаграммами, столбцами и фильтрами для каждой функции разных модулей Safetica.
- *Пользовательские* — здесь представлены отчеты, созданные пользователями Safetica для разных

функций.

- *Специальные* — здесь есть несколько специальных наборов отчетов:
    - *Время использования* — отчет о длительности активного времени по выбранным категориям приложений. Пользователь может выбирать нужные категории, установив флажок *Время использования*.
    - *Обзор* — в этот отчет включается базовая обзорная информация о функциях Safetica.

В списке выберите отчеты, которые вы хотите включить в общий отчет. После этого нажмите *Далее.*

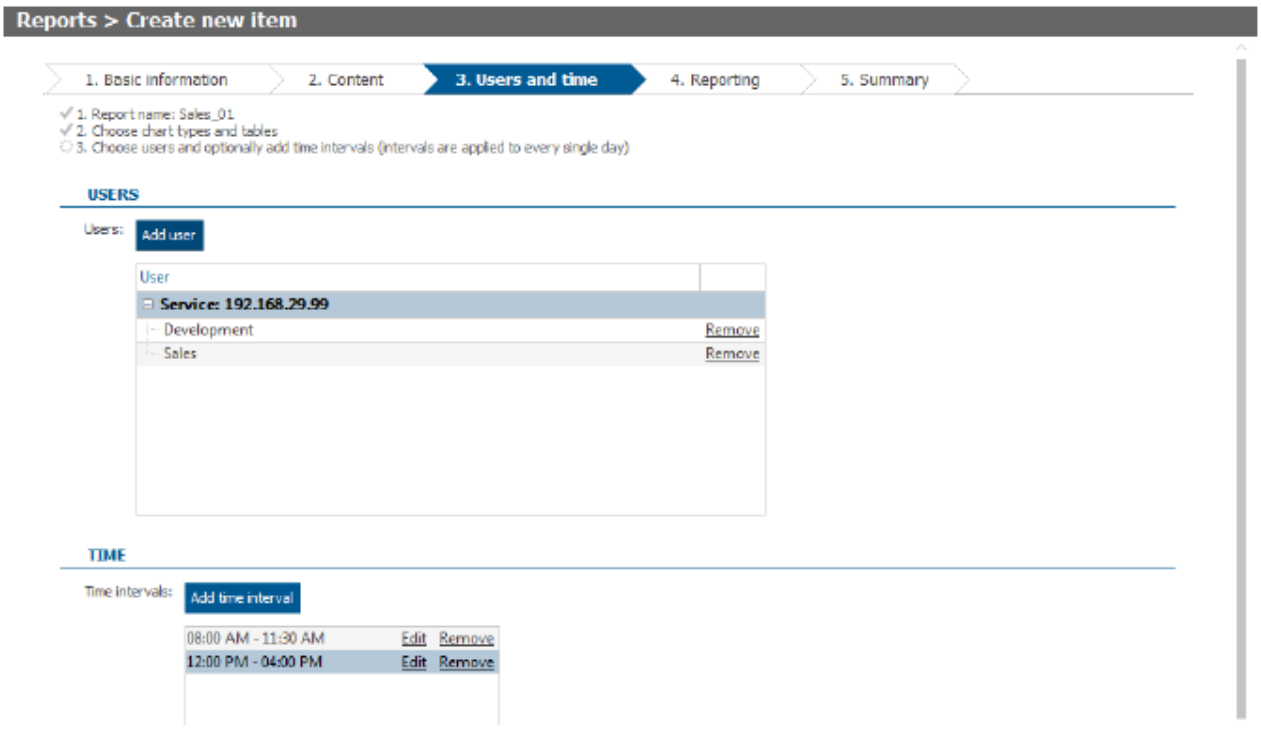


4. На следующем шаге нажмите *Добавить пользователя*. Появится диалог, в котором вы сможете выбрать компьютеры, группы или отдельных пользователей. Отчеты, которые вы выбрали на предыдущем шаге, будут впоследствии отправлены только тем пользователям, компьютерам или группам, которые вы выберете на этом шаге.

   Примечание. В отчете по умолчанию отображаются только пользователи, компьютеры и группы с выбранного сервера.

   В разделе *Время* можно указать дату отчета. Отчеты будут создаваться только из записей, созданных в указанные временные интервалы в течение дня. Если список интервалов пуст, будут использоваться данные за весь день.

   Нажмите *Далее*.



5. На предпоследнем этапе укажите, как часто и каким образом будут создаваться отчеты.

   a. Нажмите *Добавить email*, чтобы добавить адрес электронной почты, на который будет направлен созданный отчет.

   b. Используйте ползунок, чтобы выбрать форму отчетов, а также формат, в котором будет отправлен созданный отчет.

      I. *Диаграммы (pdf)* — отчеты отправляются только в форме диаграмм в формате pdf.

      II. *Журналы (xls)* — отчеты отправляются только в форме записей в таблице Excel.

      III. *Диаграммы (pdf) и журналы (xls)* — отчеты отправляются в форме диаграмм в формате pdf и записей в таблице Excel.

   c. Выберите, хотите ли вы сохранять отчеты в файл на диске. Если да, укажите путь для сохранения отчета. Отчет будет храниться на компьютере, на котором работает сервер. Указанный путь должен существовать на этом компьютере. При создании отчетов по нескольким серверам на всех компьютерах, где установлен сервер, должен существовать путь для создания отчетов.

   d. На предпоследнем этапе укажите, будет ли отчет отправляться с постоянными интервалами, или нет. Вы можете выбрать один из следующих вариантов:

      I. *День.* Отчет будет отправляться ежедневно после полуночи. Отчет содержит данные за последний день.

      II. *Неделя.* Отчет будет отправляться каждый понедельник после полуночи. Отчет содержит данные за последнюю неделю.

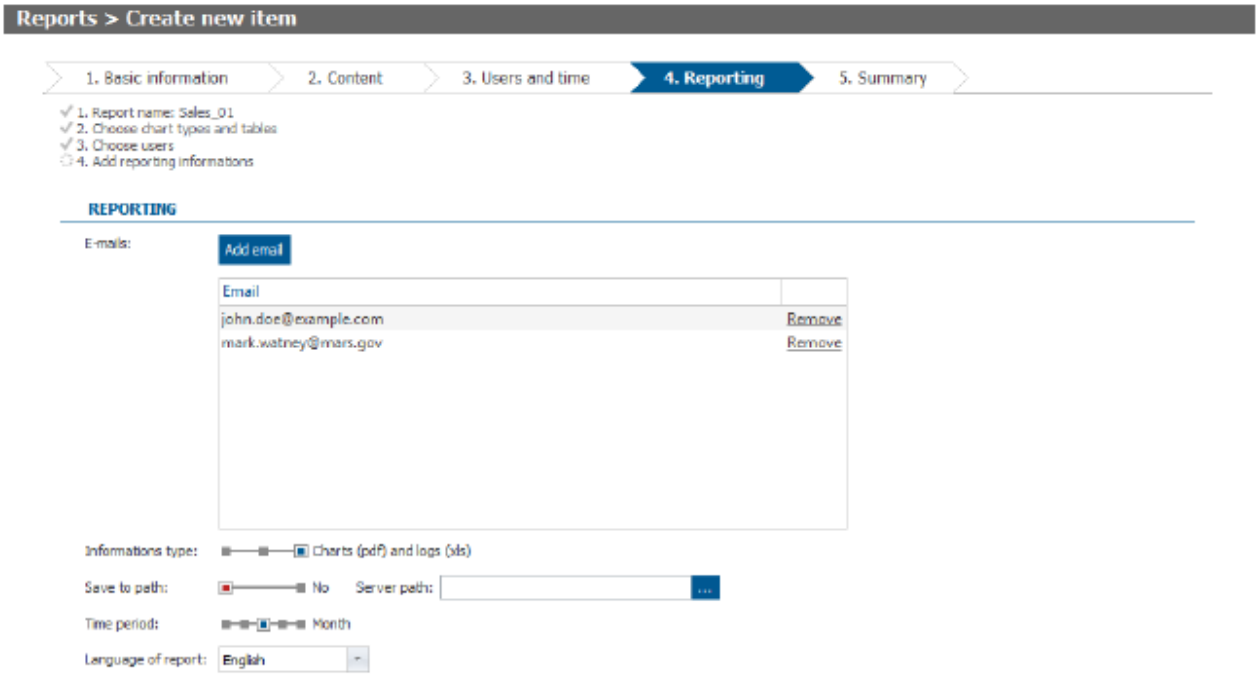
      III. *Месяц.*Отчет будет отправляться в первый день месяца после полуночи. Отчет содержит данные за последний месяц.

      IV. *Квартал.* Отчет будет отправляться 1 января, 1 апреля, 1 июля и 1 октября после полуночи. Отчет содержит данные за последний квартал.

      V. *Полугодие.* Отчет будет отправляться 1 января и 1 июля после полуночи. Отчет содержит

данные за последние 6 месяцев.

e. И наконец, выберите язык отчета. После завершения нажмите *Далее.*



6. На последнем этапе отображается обзор настроек, которые вы создали при настройке отчета. Чтобы добавить отчет к списку, щелкните по кнопке *Конец.* Для сохранения изменений нажмите на кнопку  в правой верхней части.

4.4.4. Обслуживание

4.4.4.1. Обзор конечных точек

В этом разделе вы найдете обзор конечных точек, например, их общее число, число конечных точек с установленным клиентом Safetica или с установленным агентом загрузчика.

Ниже размещается таблица с подробной информацией о конечных точках, клиенте Safetica и агенте загрузчика.

Каждая запись содержит следующую информацию:

- *ПК* — имя конечной точки, на которой установлен клиент.
- *Версия клиента* — номер установленной версии клиента.
- *Версия агента* — номер версии агента загрузчика.
- *Последнее обновление настроек* — последняя синхронизация настроек клиента.
- *Операционная система* — версия операционной системы на конечной рабочей станции.
- *Сетевой уровень* — тип используемого Safetica сетевого уровня (см. Настройки интеграции).
- *Незарегистрированные записи* — содержит количество записей от клиентов, которые еще не отправлены на сервер, и информацию об актуальности этих записей.
- *Последняя отправка журналов* — дата и время, когда клиент в последний раз отправлял записи в базу данных.

- *IP-адрес* — адрес ПК, на котором установлен клиент.
- *Сертификат отклонен* — сертификат нового сервера, отклоненный клиентом.
- *Редакция ОС*— выпуск операционной системы.
- *Service pack* — пакет обновления для операционной системы.
- *Тип операционной системы* — 32 или 64-битная архитектура.
- *Сведения о системе*— подробная информация об операционной системе.
- *Загрузить все журналы* — принудительная отправка всех записей в центральную базу данных для соответствующего клиента. Этот вариант доступен только в том случае, если на клиенте существует более 100 неотправленных записей.
- *Состояние установки* — состояние установки или обновления клиента.
- *Конфликтующее ПО* — список приложений, установленных на компьютере, которые могут конфликтовать с Safetica.
- *.NET* — наличие Microsoft.NET Framework на конечной рабочей станции.
- *Повторная установка* — перезапуск установки/обновления на конечной рабочей станции, если она не была успешно выполнена ранее.
- *Служба установлена* — наличие клиентской службы Safetica, входящей в состав клиента, на конечной рабочей станции.
- *Служба запущена* — выполнение клиентской службы Safetica на конечной рабочей станции.
- *Подключение к базе данных* — состояние подключения клиента к базе данных после ее установки.
- *Версия Webdetector* — номер используемой версии Webdetector.
- *Тип компьютера* — настольный или ноутбук.
- *Номер сборки* — номер сборки операционной системы.
- *Отсутствует ПО* — отсутствует необходимое программное обеспечение или компоненты, необходимые для корректной работы клиента или одного из его компонентов.
- *Активность в домене* — активность конечной точки в Active Directory.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.4.4.2. Обновление и развертываание

В этом разделе вы можете установить и управлять клиентом на конечных точках. Вы также можете узнать о доступных обновлениях сервера и конечных точек и установить их.

Обновление сервера

Этот раздел используется для обновлений сервера Safetica. Обновление до текущей версии выполняется щелчком по кнопке *Загрузить и обновить до версии*. Обновление выполняется для сервера, выбранного в дереве пользователей.

Регистрация конечных точек

Здесь вы можете установить, обновить и управлять клиентами на всех подключенных конечных точках.

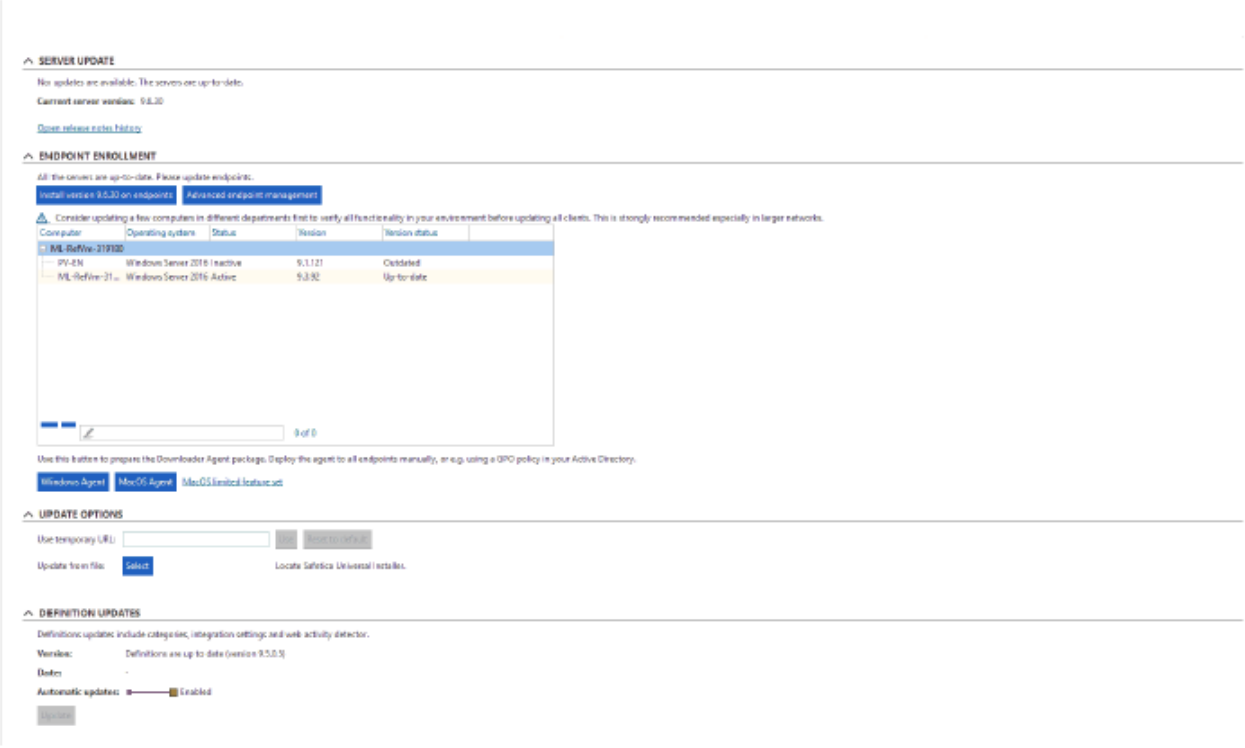
Если вы хотите установить клиент на новый компьютер, нажмите *Агент Windows* или *Агент macOS* (в зависимости от операционной системы новой конечной точки). Будет загружен установочный пакет загрузчика, и вы сможете установить его на новый компьютер. После подключения к серверу установите

клиент с помощью кнопки *Установить версию на конечные точки*. При нажатии на эту кнопку можно также обновить клиент.

Вы можете выбрать удаленную расширенную установку, обновление и удаление клиентов на подключенных конечных точках, нажав кнопку *Расширенное управление конечными точками*.

Примечание. Клиентом можно управлять только на тех конечных точках, на которые установлен агент загрузчика.

Управление конечной точкой настраивается для сервера, выбранного в дереве пользователей. Чтобы применить настройки, необходимо сохранить изменения с помощью кнопки ✓. Вы можете отменить изменения, используя кнопку ✕ в правом верхнем углу.



Расширенное управление конечными точками

Нажав на эту кнопку, вы можете установить, обновить или удалить клиент или агент загрузчика на конечных точках.

В таблице представлен список созданных задач по администрированию. Для каждой задачи в таблице, в зависимости от ее типа, можно редактировать некоторые параметры:

- Для типа *Установка/Обновление*:
  - Установка/обновление… – с помощью этой функции устанавливается или обновляется клиент. При обновлении клиента также обновляется агент загрузчика.

    Примечание. Установка или обновление удаленного клиента возможны только в том случае, если агент загрузчика установлен на конечной точке. Установка агента загрузчика на конечную точку возможна только локально или с помощью средства массовой установки (например, групповой политики Active Directory).

  - Обновить агент загрузчика.

- Для задачи *Удалить* вы можете использовать слайдер, чтобы указать, следует ли удалить только клиент или агент загрузчика тоже.

После выполнения любого типа задач вы можете использовать слайдер для принудительного перезапуска конечной точки по завершении операции.

Приводится основная статистика о статусе каждой задачи:

- Сколько компьютеров будут выполнять задачу
- Сколько компьютеров успешно выполнили задачу
- Сколько компьютеров не смогли выполнить задачу
- Сколько компьютеров ожидают перезагрузки
- Сколько компьютеров еще не выполнили задачу

Чтобы удалить задачу, используйте кнопку *Удалить*. Все выполненные задачи остаются в таблице, пока вы не удалите их вручную.

Установка или обновление

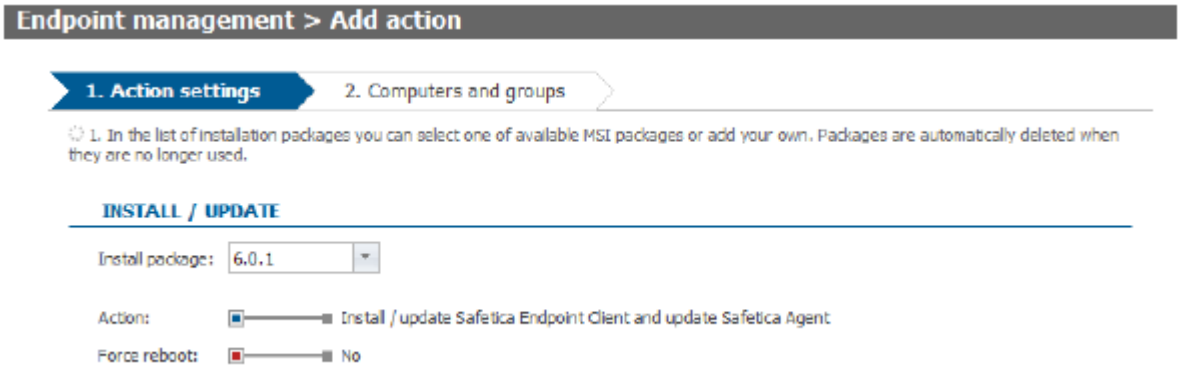
Чтобы начать установку или обновление клиента или агента загрузчика, нажмите *Install/Update.*

1. На первом шаге используйте раскрывающийся список для выбора номера версии для установки или обновления.

   Далее выберите тип задачи:

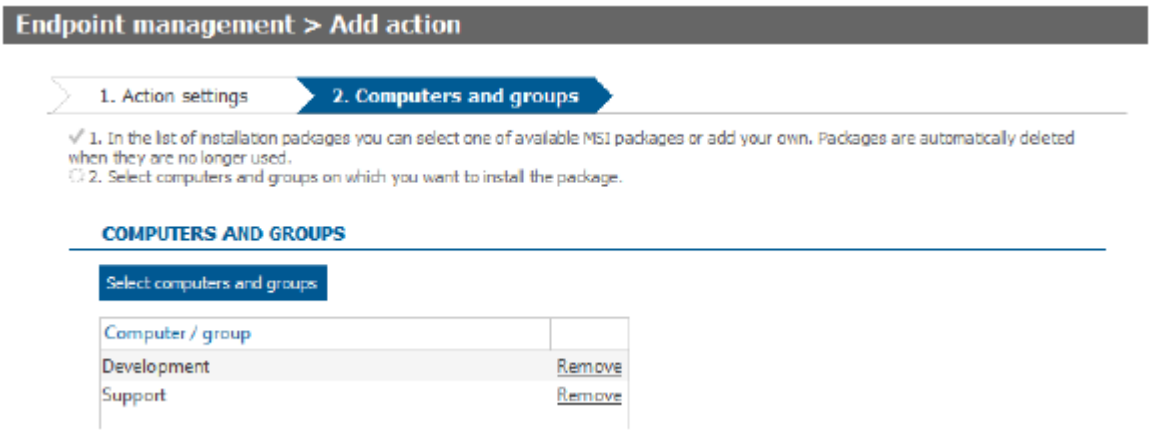
   - Установка или обновление клиента Safetica и обновление агента загрузчика
   - Обновление агента загрузчика

   В конце первого шага выберите, нужно ли перезапускать рабочую станцию после выполнения задачи.



2. На втором шаге введите группы или компьютеры, на которых будет выполняться задача. Для завершения нажмите *Конец* и сохраните задачу кнопкой  .

   Примечание. Компьютеры с назначенными задачами будут выделены.



Удаление

Чтобы начать удаление клиента или агента загрузчика, нажмите *Удалить.*

1. На первом шаге вы должны выбрать компоненты, которые хотите удалить:
   - клиент Safetica
   - клиент Safetica и агент загрузчика

Внимание! Удаление агента загрузчика отменяет установку удаленного клиента и его управление на конечной рабочей станции.

2. На втором шаге введите группы или компьютеры, на которых будет выполняться удаление. Для завершения нажмите *Конец* и сохраните задачу кнопкой ✓.

Опции обновления

В этом разделе можно указать, как будут выполняться обновления.

Текстовое окно *Использовать временный URL* используется для ввода альтернативного адреса для обновления файлов. Нажав на кнопку *Использовать*, вы загрузите установочные файлы с адреса, который вы ввели. Щелкните *Восстановить значение по умолчанию*, чтобы отменить использование альтернативного адреса.

Вы можете использовать кнопку *Выбрать* в разделе *Обновить из файла*, чтобы выбрать *универсальный установщик Safetica* с локального сайта, который будет использоваться для обновления.

Обновление определений

Здесь вы можете включить автоматическое обновление определений. Обновление относится только к изменениям в категориях, настройках интеграции, отслеживании сетевой активности и словарей.

Нажмите на кнопку *Обновление* для ручного обновления.

Примечание. Автоматическое обновление может увеличить нагрузку на SQL Server.

Визуализация

В режиме просмотра визуализаций вы можете проверить данные об успешных и неудачных обновлениях. Если в процессе обновления произойдет какая-то ошибка, вы сможете просмотреть подробное описание ошибки

рядом с соответствующей записью, нажав на ссылку *Больше информации*. После открытия этой записи вы сможете скопировать текст в буфер обмена, нажав на кнопку копирования. Затем вы сможете отправить подробную запись в службу технической поддержки, где вам помогут идентифицировать и, возможно, решить возникшую проблему.

4.4.4.3. Деактивация рабочего места

В этом режиме вы можете отключать отдельные функциональные компоненты клиента Safetica.

Примечание. Если вы хотите изменить настройку, сначала проконсультируйтесь в службе технической поддержки.

Деактивация рабочих мест выполняется на консоли в меню *Обслуживание -> Деактивация клиента*

Настройки

Функция деактивации устанавливается только для пользователей, групп, компьютеров или серверов, выбранных в дереве пользователей. Чтобы применить настройки, нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  справа вверху. Если для любой функциональной части клиента настроено отключение для любого из зарегистрированных пользователей, то клиент отключается для всей конечной станции.

Основные настройки

- *Safetica Client* — этот слайдер отключает все функции клиента (драйверы, интегрированные технологии и службы). Чтобы полностью отключить клиент, необходимо перезагрузить рабочую станцию. При этом клиент останется работать, но только для ожидания повторной активации. Чтобы посмотреть, какие компоненты Safetica Client деактивированы, проверьте пункт *Визуализация* -> таблицу *Записи* -> столбец *Деактивированные компоненты*.

Встроенные технологии

Здесь вы можете выключить (деактивировать) некоторые части Safetica.

- *Сетевой уровень* — сетевой уровень, используемый некоторыми функциями Safetica для сетевого взаимодействия. Отключение сетевого уровня повлияет на работу некоторых функций Safetica.
- *Расширение MAPI* — этот ползунок отключает расширение Safetica для клиента электронной почты Microsoft Outlook. Это расширение требуется для правильной работы мониторинга коммуникации через клиент Outlook. Для применения настроек вам нужно перезапустить Outlook на клиентской станции.

  Примечание. После отключения расширения MAPI прекращает работу только функция мониторинга электронных писем, отправляемых через Microsoft Exchange. Мониторинг электронной почты через другие протоколы будет продолжаться.

- *Контекстное меню* — вы можете отключить интеграцию некоторых функций Safetica в контекстные меню системы Windows.

Драйверы

В этом разделе вы можете удалить (отключить) драйверы, которые Safetica установила в системе. Удаление драйверов повлияет на работу функций Safetica, которые используют их.

- *Драйвер диска Safetica* — этот драйвер Safetica использует для некоторых функций взаимодействия с файловой системой. При его отключении невозможна работа следующих функций Safetica:
  - отключается защита папок установки клиента. Подробнее см. *Защита от неавторизованных действий с клиентом Safetica*.
  - *Администрирование устройств*
  - *Правила DLP*
  - *Защита диска*
- *Safetica device driver* — этот драйвер используется некоторыми функциями Safetica для управления устройствами.

Параметр *Удалить* полностью удаляет драйвер Safetica. Параметр *Деактивировать* переключает драйвер в пассивный режим, но он остается установленным.

Если вы хотите быть на 100% уверены, что проблема с устройством не связана с Safetica, вы можете попробовать удалить драйвер. В остальных случаях достаточно деактивировать его.

Для отключения драйверов нужно перезапустить рабочую станцию.

Службы

В этом разделе можно отключить службы, поддерживающие работу некоторых функций Safetica.

- *Safetica net monitor service* — поддерживает работу Safetica с сетью.
- *Safetica DLP service* — обеспечивает защиту от утечки данных в Safetica.
- *Служба мониторинга файлов Safetica* — обеспечивает отслеживание файлов (Файлы, Правила DLP).
- *Служба классификации Safetica* — обеспечивает анализ файлов и присвоение меток.
- *Служба приложений Safetica* — обеспечивает блокировку приложений.
- *Обслуживание устройств Safetica* — обеспечивает мониторинг и блокировку устройств.
- *Safetica user interaction service* – отслеживает все действия пользователя в окнах приложений и отображает всплывающие окна.
- *Safetica content analysis service* – сканирует содержимое файлов и анализирует их конфиденциальность.
- *Safetica information service* – сервисы телеметрии для анализа информации с конечных точек.

Расширенные

- *Safetica event log service – собирает события для отладки из компонентов Safetica.*

Визуализация

В режиме визуализации представлен обзор подключенных и отключенных компонентов клиента на конечных рабочих станциях.

В верхней части отображается сводная информация о количестве полностью или частично отключенных клиентов. В нижней части есть таблица с подробным перечислением включенных и отключенных компонентов клиента на рабочих станциях.

4.4.4.4. Настройки интеграции

Настройки интеграции определяют поведение Safetica на рабочих станциях. Настройки интеграции находятся на консоли в меню *Обслуживание -> Настройки интеграции*.

Режим интергрции

Вы можете выбрать один из нескольких режимов интеграции, при этом каждый из них включает все функции и возможности предыдущего (более низкого) уровня режима. Самый низкий уровень обозначается как *Без интеграции,* а самый высокий из доступных — *Максимальная интеграция*. Переключая режим интеграции, вы можете включать или отключать некоторые приложения, кроме тех, для которых настройки устанавливались вручную. Интеграция не влияет на функции модуля Discovery.

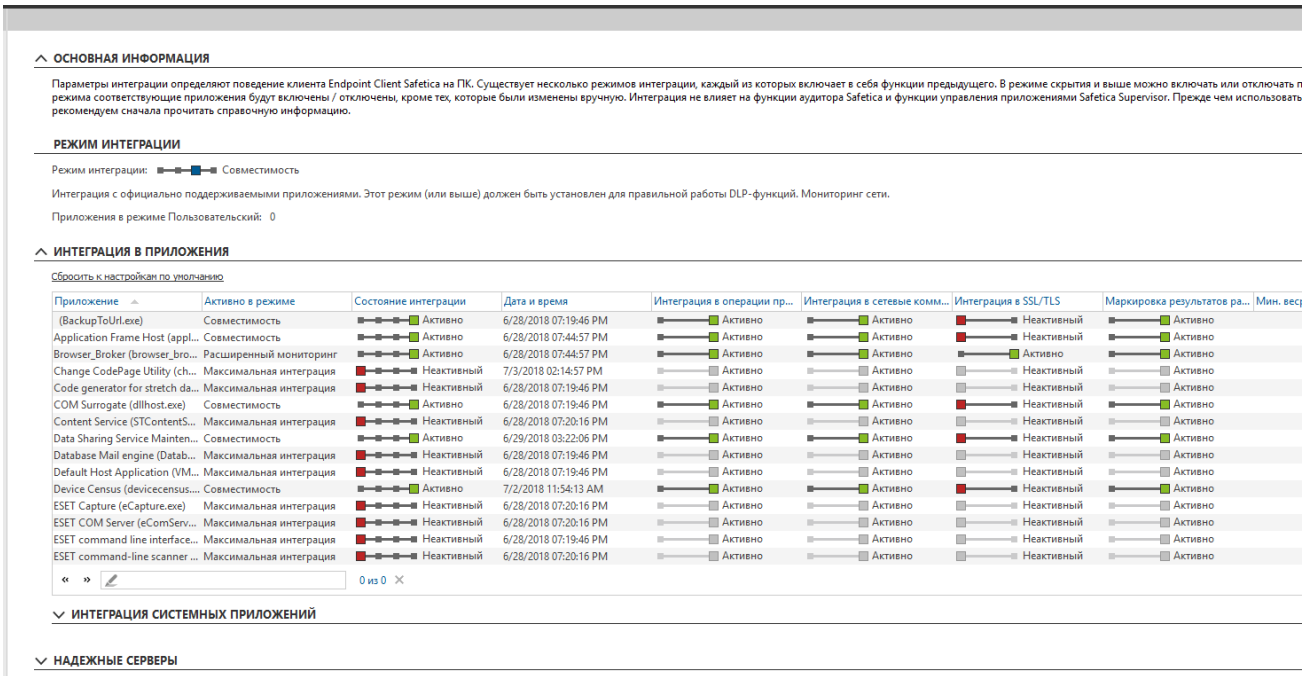
Вы можете выбрать один из следующих режимов интеграции:

- *Без интеграции* — приложения не интегрируются.
- *Расширенный мониторинг* — применяются интегрированные приложения, поддерживающие мониторинг операций с файлами и получение более качественных результатов функции Файлы. Они никак не влияют на сетевое взаимодействие.
- *Совместимость* — интеграция применяется для всех официально поддерживаемых приложений. Этот или более высокий режим требуются для правильной работы функции защиты от утечки данных (DLP). Сетевая коммуникация отслеживается.
- *Максимальная интеграция* — интеграция применяется для всех приложений за исключением тех, которые считаются несовместимыми, например, антивирусных программ. Этот режим может значительно влиять на функциональность рабочей среды. Сетевая коммуникация отслеживается.

Управление интеграцией настраивается для сервера, выбранного в дереве пользователей. Чтобы применить эти настройки, нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  справа вверху.

При индивидуальных изменениях настроек интеграции рекомендуется консультироваться со службой поддержки.

Мы рекомендуем обсуждать все изменения в настройках интеграции с технической поддержкой.



Интеграция приложений

В этом разделе есть два списка приложений. Первый содержит все несистемные приложения, обнаруженные на рабочей станции. Эти приложения интегрируются в соответствии с выбранным режимом интеграции. В скрытом или более высоком режиме есть возможность вручную включать и отключать интеграцию каждого приложения.

Список содержит следующую информацию:

- *Приложение* — название приложения
- *Дата и время* — дата и время обнаружения приложения.
- *Активно в режиме* — определяет, начиная с какого режима активируется интеграция этого приложения. Если здесь выбран вариант *Пользовательский,* значит интеграция включена вручную.
- *Состояние интеграции* — здесь вы можете указать режим интеграции для конкретных приложений:
  - *Неактивный* — приложение не интегрируется.
  - *Неактивно (Активно в тестовой группе)* — приложение интегрируется только на компьютерах, включенных в тестовую группу (см. раздел *Тестовая группа* ниже).
  - *Активно (Неактивно в тестовой группе)* — приложение интегрируется на всех компьютерах, кроме включенных в тестовую группу.
  - *Активно* — интеграция включена на всех компьютерах.

Следующие опции позволяют включить или отключить интеграцию в отдельных функциональных частях приложения. Вы можете включить или отключить интеграцию в частях приложения.

- *Интеграция в операции приложения* - если интеграция активна, Safetica сможет контролировать внутренние операции приложения и/или вмешиваться в такие операции с целью обеспечения безопасности. Это может произойти, например, в принудительной политике безопасности.
- *Интеграция в сетевые коммуникации* - если интеграция активна, Safetica сможет контролировать все сетевые коммуникации и/или вмешиваться в такие коммуникации с целью обеспечения безопасности. Это может произойти, например, в принудительной политике безопасности.

- *Интеграция в SSL/TLS* - если интеграция активна, Safetica сможет контролировать все зашифрованные коммуникации SSL/TLS и/или вмешиваться в такие коммуникации с целью обеспечения безопасности. Это может произойти, например, в принудительной политике безопасности.
- *Маркировка результатов работы приложения* - если интеграция активна, Safetica сможет отслеживать действия приложения и непрерывно маркировать свои выходные данные на основе применимых политик безопасности.

Нажмите *Сбросить к настройкам по умолчанию* над списком, чтобы применить для всех приложений в списке настройки по умолчанию.

Добавление нового приложения

Каждое приложение, установленное на конечных станциях, синхронизируется со списком на консоли. Если вы хотите предварительно создать настройки для приложения, которое еще не было обнаружено на конечной станции, в *Категории > Просмотр базы данных > Добавить приложение*. В диалоговом окне выберите файл .exe того приложения, которое вы хотите добавить. Файл процесса приложения должен быть доступен со станции, на которой в настоящий момент запущена консоль. После подтверждения Safetica загружает информацию, необходимую для правильной идентификации приложения во всех системах.

Системные приложения

В таблице перечислены важные приложения операционной системы. Для этих приложений настроены определенные параметры интеграции; не рекомендуется изменять эти параметры. Изменение поведения может влиять на функциональность рабочей среды.

Доверенные серверы

Вы можете использовать таблицу в расширенных настройках интеграции SSL, чтобы добавлять новые веб-сайты, с которыми Safetica необходимо поддерживать защищенную связь по протоколу SSL/TLS. Новые веб-сайты добавляются в список с помощью кнопки *Добавить адрес*.

Проблемные устройства

Более подробная информация доступна в базе знаний Safetica.

Тестовая группа

Тестовая группа компьютеров предназначена для проверки правильности взаимодействия Safetica с различными приложениями. Добавляйте в тестовую группу только те компьютеры, программное и аппаратное обеспечение которых в точности соответствует типичным характеристикам в вашей среде. Кроме того, не следует добавлять в нее компьютеры, которые критически важны для работы инфраструктуры и/или содержат конфиденциальные данные. Применение интеграции Safetica на компьютерах, входящих и не входящих в эту группу, подробно описано выше, в разделе о настройках интеграции для конкретных приложений.

Чтобы добавить компьютер в этот список, нажмите *Добавить компьютер* и в диалоговом окне отметьте нужные компьютеры. Подтвердите свой выбор кнопкой *ОК*.

Системные пути

В разделе *Обслуживание -> Настройки интеграции -> Системные пути* вы можете указать ссылки, которые Safetica будет обрабатывать как системные по умолчанию (это, в частности, папки с файлами ОС,

установленными приложениями или временными файлами запущенных приложений).

Примеры системных папок и подпапок по умолчанию:

- C:\System Volume Information
- C:\Users\<User name>\AppData
- C:\Program Files
- C:\Program Files (x86)
- C:\Windows

Файловые операции для этих папок не регистрируются. Чтобы добавить свою собственную ссылку по умолчанию, нажмите на кнопку *Добавить путь* и введите ссылку на папку. Все подпапки тоже будут считаться системными.

Вы также можете использовать системные ссылки для разметки файлов. Перейдите к правилам приложения в категории **контекстных** данных (*Защита -> Категории данных -> Настроить категорию данных -> Правила приложений -> Добавить -> Дополнительно -> Включить систему*), где вы можете выбрать включение тегирования системных файлов. По умолчанию эта опция отключена.

Интеграция с Office 365

Safetica 9.5 и более поздних версий автоматизирует настройку аудита и DLP для электронной почты и файлов, хранящихся в облаке. Функциональность DLP доступна в Safetica Protection и Safetica Enterprise. Safetica Discovery поддерживает функции аудита.

Более подробная информация доступна в базе знаний.

Интеграция с FortiGate

Интеграция с решениями для сетевой безопасности FortiGate доступна в Safetica Enterprise.

Более подробная информация доступна в базе знаний.

Сетевые сертификаты

Safetica выполняет проверку SSL на конечных точках для защиты данных в зашифрованном сетевом соединении. Также выполняется проверка сетевого сертификата. Вы можете настроить параметры проверки:

- *Полная* – все ошибки, связанные с ненадежными сертификатами, отображаются на конечной точке.
- *Умеренная* – режим по умолчанию. Некоторые ошибки ненадежных сертификатов игнорируются.
- *Полная настраиваемая* – позволяет синхронизировать проверку SSL на конечной точке с проверкой сети. Здесь вы можете импортировать сертификаты, используемые вашим решением для сетевой безопасности. После импорта сертификаты распространяются на все конечные точки, на которых работает Safetica. После подключения к корпоративной сети (и серверу Safetica) продукт расшифровывает только те SSL-соединения, которые также расшифровываются вашим решением для сетевой безопасности.

Примечание. Целью дешифровки является исключительно проверка связи на предмет защиты от утечек. Коммуникации повторно шифруются после проверки.

4.4.4.5. Настройки клиента

К настройкам клиента относится общая конфигурация клиента Safetica.

Настройки

Настройки клиента устанавливаются только для пользователей, групп, компьютеров или серверов, выбранных в дереве пользователей. Чтобы применить настройки, нужно сохранить изменения с помощью кнопки ✓. Также вы можете отменить изменения кнопкой ✕ справа вверху.

Разрешенные действия

С помощью функций *Удаление* и *Обновление* можно соответственно удалить или обновить клиент. Без такого разрешения невозможно удалить, обновить или иным образом вмешаться в работу клиента из соображений безопасности, даже имея права администратора. Вы можете использовать кнопку пароля для настройки нового пароля на разрешение этих задач непосредственно с клиентской станции, с помощью командной строки. Более подробная информация о защите клиента Safetica приводится в разделе *Защита от несанкционированных манипуляций клиента*.

Вы можете запретить все действия, разрешенные локально, нажав *Отключить действия локального управления*.

Общие настройки интерфейса

- *Скрывать процессы и папки Safetica*. Если вы активируете эту функцию, процессы STCSer.exe, STMonitor.exe, STUserApp.exe и STPCLock.exe, обеспечивающие работу клиентской службы Safetica Client Service, будут скрыты на клиентской станции и не будут отображаться в диспетчере задач Windows или в любой аналогичной программе, которая отслеживает запущенные процессы. Клиент не будет виден в списке *установленных программ*. Папки установки и настроек клиента также будут скрыты (в Windows 7: *C:\Program Files\Safetica*, *C:\ProgramData\Safetica* и *C:\ProgramData\Safetica Client Service*). Таким образом вы не позволите пользователям узнать, что Safetica работает на их компьютерах. Эта функция не отключает диалоговые окна уведомлений.
- *Уведомление клиента.* Эта функция включает и отключает отображение диалоговых окон с оповещениями для пользователей, работающих на клиентских компьютерах. Диалоговые окна с оповещениями информируют пользователей о различных событиях, связанных с безопасностью, либо о запрещенной активности. Есть несколько способов настроить отправку оповещений:
  - Скры*ть все* — все диалоговые окна клиента будут спрятаны.
  - *Показать только интерактивные диалоги* — будут спрятаны все диалоги, кроме тех, которые

требуют взаимодействия с пользователем.

- *Показать все* — все диалоги будут отображаться.

- *Язык.* Настройка языка клиента.

Другие настройки

- *Настройка приоритетов политик.* Настройка повышает приоритет настроек, которые вы установили для пользователя, над настройками компьютера, с которого подключился пользователь. По умолчанию приоритет будет у настроек компьютера. Вы можете установить такой приоритет только для пользователей.

- *Интервал для отправки журналов.* Эта настройка определяет, как часто данные, записываемые на клиентских станциях, будут группироваться в пакеты и отправляться для сохранения в базе данных. При накоплении большого количества записей интервал отправки автоматически сократится. После сокращения количества собранных записей интервал отправки возвратится к первоначальному значению.

- *Интервал проверки настроек.* Эта настройка определяет, как часто клиент будет запрашивать новые настройки на сервере. Таким образом вы можете повлиять на время, необходимое для передачи клиенту настроек, выполненных с помощью консоли.

- *Время, затраченное на отправку журналов.* Здесь вы можете указать, какой процент времени уходит на отправку клиентских записей в базу данных. Более низкие значения предотвратят чрезмерную нагрузку на сеть.

  Примечание. Значение по умолчанию — 10 %. Его не следует менять без достаточного основания и соответствующих знаний. Если вы все равно хотите изменить настройку, сначала проконсультируйтесь в службе технической поддержки.

- *Интервал определения неактивности пользователя.* Здесь можно указать временной интервал, по истечении которого оценка статуса активности пользователя изменится с активного на неактивный. Другими словами, если пользователь не работает со своим ПК (не использует мышь или клавиатуру) в течение этого периода времени, статус его измеренной активности изменится на неактивный. Эти настройки влияют на измерение активного времени в функциях раздела Приложения и тенденции модуля Safetica UEBA.

- *Безопасный режим.* Выбрав запретить, вы можете запретить пользователям запускать Windows в безопасном режиме.

Отчет об ошибках

Здесь можно установить уровень ведения журнала отладки клиента: от ошибок до максимально подробных данных. Этот параметр предназначен для использования системными администраторами или технической поддержкой Safetica. Подробный уровень ведения журналов может негативно отразиться на производительности клиента.

Уведомления

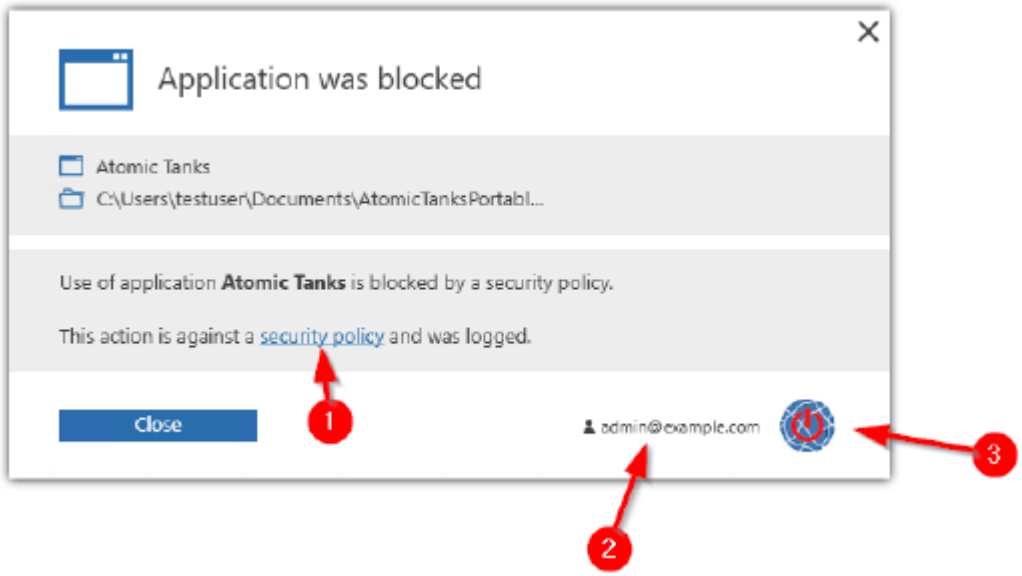
Функция доступна в Safetica Protection и Safetica Enterprise. Вы можете частично настроить внешний вид диалоговых окон оповещений, отображаемых для пользователей:

1. *Логотип для окна уведомления* — заменяет логотип для диалогового окна по умолчанию на ваш собственный. Выбранный логотип должен иметь размеры 92 x 62 пикселя и формат .png, .jpg или .bmp.

2. *Контактный e-mail* — адрес электронной почты, который будет отображаться внизу диалогового окна.
3. *Политика безопасности* — URL-адрес вашей политики безопасности.

Настройки:

Полученный в результате диалог оповещения с подробной информацией, которая будет отображаться для пользователей:



Более подробную информацию можно получить в разделе справки *Диалоги оповещений*.

Классификация данных на основе пользователей

Функция доступна в Safetica Protection и Safetica Enterprise. Более подробная информация доступна в базе знаний.

Нерабочие часы

Функция доступна в Safetica Protection и Safetica Enterprise, а также в модуле Safetica UEBA. С помощью этих настроек вы можете отрегулировать режим работы Safetica в нерабочее время. Эти настройки повлияют на мониторинг и блокировку приложений и веб-сайтов. Защита данных будет функционировать всегда, независимо от локальной настройки рабочего времени.

С помощью переключателя можно выбрать один из следующих режимов работы Safetica в нерабочее время:

- *Мониторинг и блокировка на основе производительности.* В нерабочие часы Safetica будет вести

себя так же, как и в рабочие.

- *Не блокировано по производительности.* В нерабочее время будут отслеживаться приложения и веб-сайты, но они не будут заблокированы.
- *Мониторинг и блокировка не на основе производительности.* В нерабочее время приложения и веб-сайты не будут контролироваться или блокироваться.

Рабочие часы

Чтобы открыть подробные настройки для рабочего времени, нажмите соответствующую кнопку (*Рабочие часы*). Эти настройки применяются ко всему серверу. Вы можете указать, какие дни считаются рабочими, а также выбрать время начала и окончания рабочего дня.

Нерабочие дни

Здесь можно настроить нерабочие дни. Вы можете добавить известные праздничные дни из списка для каждой страны, собственные нерабочие дни организации и праздники, а также использовать комбинацию этих подходов.

Визуализация

Каждая запись содержит несколько типов информации, представленной в формате столбцов:

- *Дата и время* — дата и время выполнения операции локального администрирования.
- *ПК* — имя компьютера, на котором выполнялась операция.
- *Имя пользователя* — имя пользователя, под учетной записью которого выполнялась операция.
- *Действия* — выполнявшаяся локальная задача по администрированию.
- *Детали* — прочая информация о выполненной операции.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.4.4.6. Сбор отладочной информации

В этом разделе можно создавать задачи по сбору отладочной информации от клиента Safetica. Сбор отладочной информации находится на консоли в меню Обслуживание -> Информации для отладки.

Сбор отладочной информации настраивается для сервера, выбранного в дереве пользователей. Чтобы применить эти настройки, нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  справа вверху.

Настройки сбора

В этом разделе можно создавать новые задачи по сбору отладочной информации от клиента. Собранная информация будет сохранена в папке на сервере, который был указан в начале процесса настроек. Путь к собранным данным на сервере можно изменять.

Для создания новой задачи нажмите на кнопку *Добавить задачу сбора.* Откроется мастер создания задачи:

1. На первом шаге с помощью ползунка выберите информацию, которую вы хотите получить. Вы

можете выбрать один из следующих вариантов:

- *Пользовательский* — выбрав этот вариант, вы можете вручную выбрать элементы информации, собираемой с клиента. Из списка под этим ползунком выберите нужные элементы для сбора информации.
- *Продвинутый* — будет собираться более подробная информация о клиенте. Содержимое этой информации отображается под ползунком.
- *Основной* — будет собираться только самая базовая информация о клиенте. Содержимое этой информации отображается под ползунком.
- *Из SMS* – будет собираться информация из Safetica Management Service, а не с конечной точки. Вы можете использовать этот вариант для устранения проблем с сервером, на котором работает Safetica.

После выбора нажмите *Далее.*

2. На втором шаге выберите группы или компьютеры, с которых вы хотите собирать отладочную информацию о клиенте. Затем нажмите *Конец* и сохраните задачу кнопкой  .

В нижней части экрана настройки сбора информации отображается таблица с обзором существующих задач. Для каждой задачи указывается, на каком рабочем месте или в какой группе выполнялся сбор данных, какие файлы были включены в сборку, а также статус загрузки на сервер.

Для отмены задачи нажмите *Удалить*.

После нажатия кнопки *Загрузка* откроется диалоговое окно, в котором вы можете выбрать местоположение, в которое будет сохранена вся собранная отладочная информация с сервера.

Выбрав *Детали,* вы откроете окно с подробной информацией о сборе отладочной информации. Здесь вы можете загрузить отдельные файлы из коллекции.

Загрузка

В этом разделе кратко описывается загрузка собранной отладочной информации с сервера на локальную консоль. Если при загрузке произойдет ошибка, вы можете повторить процесс, нажав *Загрузить снова.*

Нажав *Удалить завершенные загрузки*, вы удалите все записи о завершенных операциях сбора отладочной информации.

Визуализация

В режиме визуализации таблица с записями о размере файлов вместе с отладочной информацией находится на конечных рабочих станциях. Каждая запись содержит следующую информацию (столбцы):

- *Компьютер* — имя конечной рабочей станции.
- *Изменено* — дата последнего обновления размера файла с отладочной информацией. Здесь также содержится информация о размере каждого файла с отладочной информацией.
- Также есть размеры каждого файла с отладочной информацией.

Более подробная информация доступна в разделе *Режим визуализации*.

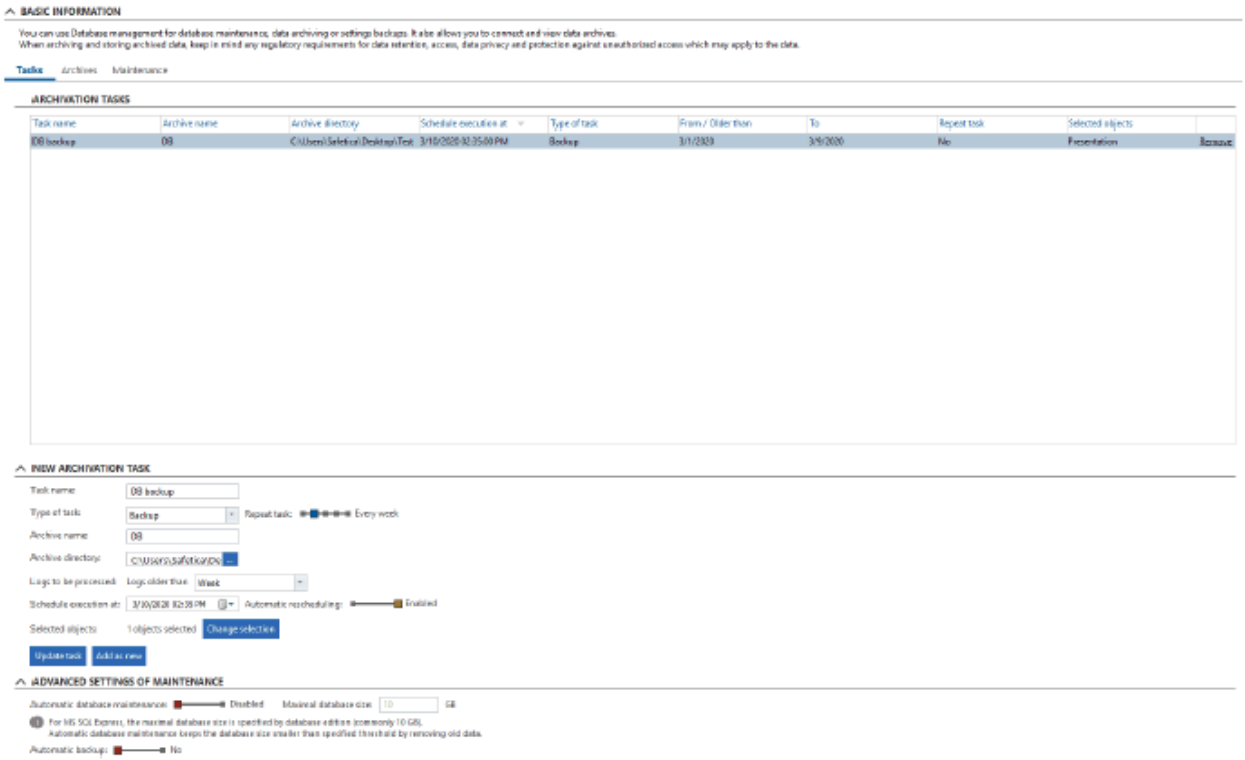
4.4.4.7. Управление базой данных

Менеджер баз данных используется для резервного копирования данных мониторинга и настроек, а также для удаления устаревших данных.

Вы управляете базами данных сервера, выбранного в дереве пользователей. Чтобы применить настройки, нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  справа вверху.

Менеджер баз данных разделен на две основные части:

- Задачи. Здесь вы можете создать задачу по резервному копированию базы данных (созданию архива) и удалению данных, созданных в процессе мониторинга.
- Архивы. С помощью этой вкладки можно подключить ранее созданные архивы к выбранному серверу, чтобы просмотреть данные.
- *Обслуживание.* Показывает информацию о базах данных всех экземпляров сервера, которыми вы управляете через консоль. Эту информацию можно экспортировать в формате XML.



4.4.4.7.1. Задачи

Задачи используются для работы с данными, которые хранятся в базе. Для этих данных можно сделать резервную копию (архив) из операционной базы данных SES, либо их можно удалить напрямую.

Все задачи создаются с помощью меню новых задач по архивированию. Новая задача имеет несколько параметров:

- *Имя задачи* — название вашей задачи.
- Тип задачи. Вы можете выбрать один из следующих вариантов: резервная копия, резервная копия с

удалением, удаление, удаление снимков экрана, настройки резервного копирования. Ниже приводится более подробная информация о каждой из задач.

- *Повторить задачу.* Указывает, как часто будет повторяться эта задача:
  - *Каждую неделю*
  - *Каждые 14 дней*
  - *Каждый месяц*
  - *Каждые три месяца*
- *Имя архива* — имя файла с резервной копией. Оно не должно содержать недопустимых символов, например пробелов. Детали по ссылке.
- *Archive directory* — путь к папке, где будет сохранен файл с резервной копией базы данных. Путь указан для компьютера, на котором работает сервер SQL. Необходимо выбрать существующий путь, поскольку сервер SQL не умеет его создавать.
- *Журналы, подлежащие обработке*:
  - С – По. Здесь вы можете выбрать период времени для резервного копирования данных мониторинга.
  - Журналы старше, чем... Обработка всех журналов старше определенной даты. Этот вариант доступен только при создании задачи удаления.
- *Выполнение запланированно на.* Установка точного времени запуска задания. Время начала задания должно находиться за пределами интервала, за который обрабатываются записи.
- *Автоматическое перепланирование.* Если включен этот параметр, функция будет автоматически назначать новое время для выполнения задания, если оно запускается одновременно с выполнением другого задания или назначается на уже прошедшее время. На одном сервере или экземпляре SQL одновременно может выполняться только одна задача, поэтому эта функция применяется только когда происходит ошибка времени. При любых других конфликтах (недостаток места на диске, отсутствие прав на запись и т. п.) новое время не назначается.
- *Выбранные объекты.* Вам обязательно нужно выбрать, для каких пользователей, компьютеров или групп будет выполняться задача резервного копирования или удаления.

Резервное копирование

Резервная копия будет создана в указанное время для выбранных пользователей, компьютеров или групп. В резервной копии будут содержаться записи мониторинга пользователей. Настройки модулей и функций не включаются в резервную копию. На выходе создается два файла: один (*.mdf) — запись базы данных, а второй (*.ldf) — журнал действий с базой данных. Каждый сервер имеет собственную базу данных, поэтому для архивирования данных из базы нужно запустить задачу резервного копирования на каждом сервере, и эти задачи будут независимы друг от друга.

При создании резервной копии сервер SQL оказывается значительно загружен, поэтому связь клиентских станций с базой данных может временно прерваться. В этой связи новые задачи следует планировать на то время, когда нагрузка на базу данных минимальна (например, ночью). Процесс может занять несколько часов. Продолжительность зависит от количества копируемых данных и размера исходной базы данных. Во время резервного копирования не рекомендуется выполнять другие действия с базой данных, например, переиндексацию, поскольку это может привести к сбою резервного копирования.

Удаление

Задача удаления выполняет удаление пользовательских настроек, журналов и снимков экрана. Будут удалены данные начиная с указанной даты. После удаления данных рекомендуется вручную выполнить команду SHRINK в базах данных Safetica SQL. Эта команда физически сожмет файл базы данных.

Расширенные настройки обслуживания

В этом разделе вы можете настроить параметры обслуживания для базы записей:

- *Автоматическое обслуживание базы данных.* Здесь вы можете указать максимальный допустимый размер записей в базе данных. При превышении этого значения некоторые записи в базе данных будут автоматически удалены, чтобы размер базы данных не превышал 70 % от установленного максимального размера. Размер проверяется ежедневно. Если вы введете, например, значение 100 ГБ в качестве максимального, размер будет уменьшен примерно до 70 ГБ.

  Внимание! Записи, удаленные в процессе обслуживания базы данных, безвозвратно теряются. Удаляются всегда самые старые записи.

- *Автоматическое резервное копирование.* Safetica каждый день около полуночи выполняет резервное копирование базы данных для предотвращения риска ее повреждения. Эта резервная копия хранится на протяжении месяца. Такие резервные копии не заменяют собой пользовательские резервные копии базы данных.

Визуализация

Визуализация задачи включает таблицу с подробными отчетами о выполняемых задачах администрирования базы данных.

Каждая запись содержит несколько типов информации, представленной в формате столбцов. Список доступных столбцов расположен в правой части таблицы. Столбец окажется в таблице после щелчка и перетаскивания его из списка в таблицу. Щелкните и переместите заголовок столбца, чтобы изменить порядок столбцов в таблице. Таким же образом вы можете перетаскивать заголовки столбцов в зону над таблицей. После этого над таблицей отобразится сводная информация по всем записям в зависимости от типа столбца. Вы можете удалить столбец из таблицы, перетащив его обратно в список столбцов, расположенный справа.

Доступные столбцы с записями о выполненных задачах:

- *Дата и время* — дата и время создания записи.
- *Имя пользователя* — имя учетной записи пользователя Safetica, которая использовалась для администрирования. После имени учетной записи указано имя компьютера, с которого выполнялась задача администрирования (<имя учетной записи>@<имя компьютера>).
- *Имя задачи*
- *Имя архива*
- *Archive Directory* — папка, в которой будет храниться архив.

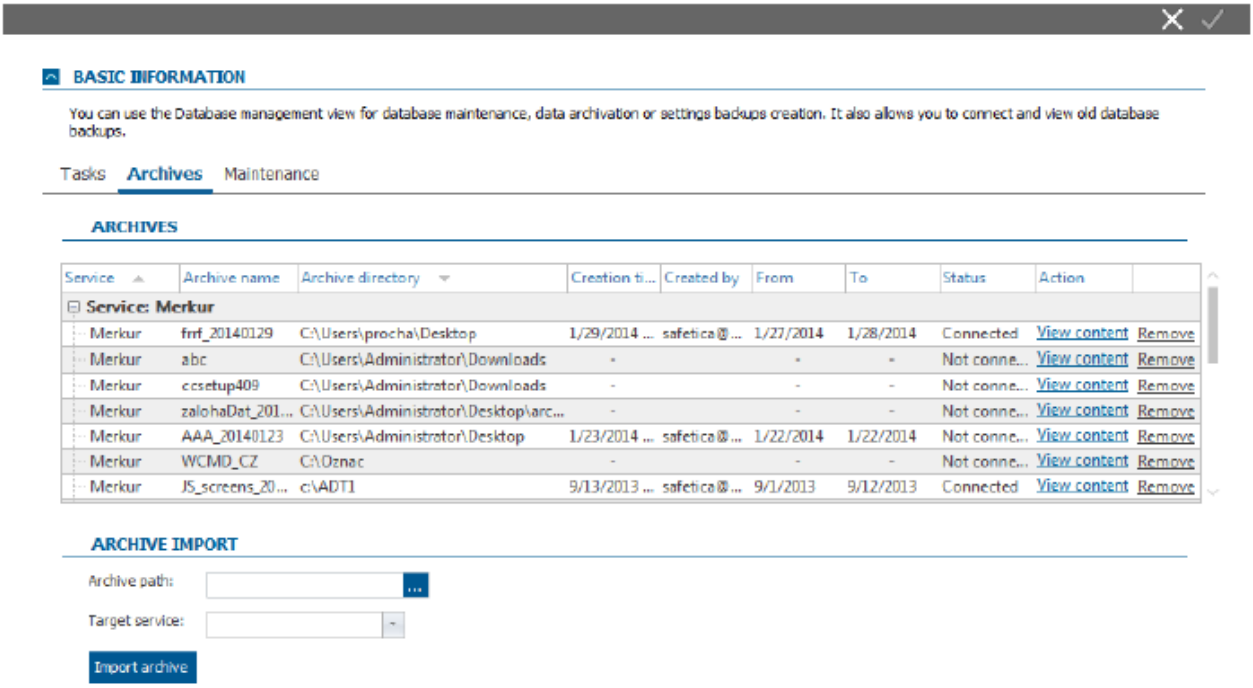
  Примечание. Это папка на компьютере с базой данных Safetica.
- *Тип задачи* — тип выполняемой задачи: резервное копирование, резервное копирование с удалением, удаление, удаление снимков экрана, резервное копирование настроек.
- Детали — подробная информация о задаче, которая будет отображаться после нажатия одноименной кнопки Детали.

Также вы можете фильтровать записи. Чтобы открыть фильтр для выбранного вами столбца, нажмите на кнопку рядом с заголовком этого столбца. Введите текст в появившемся диалоговом окне или выберите пункт из списка, чтобы фильтровать столбец по этому параметру. Чтобы добавить элемент к фильтру, щелкните по кнопке +.
Список может быть любой длины. После подтверждения фильтра нажатием кнопки ОК таблица будет отображать только те записи, которые соответствуют хотя бы одному фильтру из списка.

Вы можете узнать больше о настройках и интерфейсе визуализации в главе Журналы и визуализация.

4.4.4.7.2. Архивы

В разделе архивов отображаются ранее созданные архивы. Для просмотра необходимо подключить архив к серверу Safetica. После подключения архивы действуют как общая база записей. В этом режиме все операции настройки на консоли становятся неактивными (например, DLP не может устанавливать правила, запрещать запуск приложений и т. п.)



Импорт архива

Архив, созданный на другом сервере, можно импортировать вручную. Это делается указанием пути к архиву и целевому серверу, к которому будет подключен архив. Затем с помощью кнопки *Импорт архива* импортируйте его в список.

Просмотр архива

Вы можете подключить соответствующий архив (резервную копию) к консоли, нажав на ссылку *Просмотр содержимого*. Одновременно можно подключить несколько архивов. Каждый приложенный архив появляется как новый корневой элемент в дереве пользователей.

Закрыть архив – отключить его от сервера

Отключение архива можно выполнить в дереве пользователей или в режиме управления базой данных. Щелкните правой кнопкой мыши по имени или адресу сервера и выберите Закрыть архив. Также можно открыть База данных -> Архивы и нажать на ссылку *Закрыть архив* для конкретного архива.

Визуализация

Визуализация содержит таблицу с подробными записями о том, как обрабатывались архивы базы данных, которые были созданы.

Каждая запись содержит несколько типов информации, представленной в виде столбцов. Список доступных столбцов расположен в правой части таблицы. Столбец окажется в таблице после щелчка и перетаскивания его из списка в таблицу. Щелкните и переместите заголовок столбца, чтобы изменить порядок столбцов в таблице. Таким же образом вы можете перетаскивать заголовки столбцов в зону над таблицей. После этого над таблицей отобразится сводная информация по всем записям в зависимости от типа столбца. Вы можете удалить столбец из таблицы, перетащив его обратно в список столбцов, расположенный справа.

Для архивных записей об обработке доступна следующая информация:

- *Дата и время* — дата и время создания записи.
- *Имя пользователя* — имя учетной записи пользователя Safetica, которая использовалась для администрирования. После имени учетной записи указано имя компьютера, с которого выполнялась задача администрирования (<имя учетной записи>@<имя компьютера>).
- *Путь к архиву* — путь сохранения архива.
- *Примечание. Это папка на компьютере с базой данных Safetica.*
- *Имя сервера* — имя экземпляра сервера, к которому подключен архив.
- *Действие* — операция, выполняемая с архивом: просмотр базы данных, подключение, отключение, закрытие архива.
- *Детали.* Нажатие на эту кнопку отображает подробную информацию о том, как обрабатывался архив.

Также вы можете фильтровать записи. Чтобы открыть фильтр для выбранного вами столбца, нажмите на кнопку  рядом с заголовком этого столбца. Введите текст в появившемся диалоговом окне или выберите пункт из списка, чтобы фильтровать столбец по этому параметру. Чтобы добавить элемент к фильтру, щелкните по кнопке  .
Список может быть любой длины. После подтверждения фильтра нажатием кнопки ОК таблица будет отображать только те записи, которые соответствуют хотя бы одному фильтру из списка.

Вы можете узнать больше о настройках и интерфейсе визуализации в главе Журналы и визуализация.

4.4.4.7.3. Обслуживание

В разделе «Обслуживание» вы найдете подробную информацию об использовании основной базы данных и базы данных записей на всех экземплярах сервера, которыми вы управляете с консоли.

Нажав на кнопку *Экспорт*, вы можете сохранить сводные данные об использовании базы данных в таблицу Excel (.xls). Вместе с таблицей будет экспортирован XML-файл с таким же именем, содержащий подробную информацию о базе данных.

Отправка статистики

С помощью кнопки *Автоматическая отправка статистики* вы можете включить отправку основных статистических данных о вашей установке Safetica в Safetica Technologies. Статистика будет отправляться раз в неделю и содержать следующую информацию:

- Номер лицензии
- Версия и количество установленных клиентов Safetica
- Файл XML, содержащий подробную информацию о заполненности базы данных

Эти данные используются для улучшения продуктов и служб Safetica Technologies и не содержат конфиденциальной информации.

Сценарии обслуживания

В этом разделе пользователь может запустить сценарии обслуживания базы данных. Из соображений безопасности разрешены только сценарии, подписанные Safetica Technologies.

Сначала нужно выбрать сценарий. Это делается через диалог выбора файлов, который можно открыть кнопкой  . Нажмите *Отправить,* чтобы запустить указанный сценарий. После выполнения сценария вам будет предложено сохранить файл с выходными данными выполненного скрипта.

4.4.4.8. Управление доступом

Здесь вы можете управлять учетными записями для входа в отдельные модули сервера, а также правами доступа и настройками. Учетная запись предоставляет также доступ к консоли Safetica. Аутентификация всех учетных записей осуществляется с помощью имени пользователя и пароля.

Управление учетными записями пользователей можно найти на консоли в меню *Обслуживание -> Управление доступом.*

Настройки

В режиме просмотра настроек слева находится список учетных записей, созданных на подключенном в данный момент сервере. На правой панели отображаются права доступа к отдельным функциям и настройки для выбранной учетной записи и узла дерева.

Учетные записи пользователей

В этой части отображается список учетных записей пользователей Safetica.

Учетные записи по умолчанию:

- Учетная запись администратора службы с эксклюзивным доступом ко всем функциям и настройкам.
  - Имя: safetica
  - Пароль по умолчанию: S@fetic@2004
  - После первого входа в систему Safetica с использованием этой учетной записи пользователю будет предложено изменить пароль.
  - Эта учетная запись не может быть удалена, отключена или переименована.

    - Пароль к ней можно изменить только после входа в Safetica с этой учетной записью в меню Профиль -> Изменить пароль.
- Учетная запись с предустановленными базовыми правами на функции Safetica.
    - Имя для входа: starter
    - Эта учетная запись не может быть удалена, отключена или переименована.

Новые учетные записи можно добавить, нажав *Добавить аккаунт* и введя новое имя пользователя и пароль.

Кнопка *Клонировать* позволяет создать новую учетную запись с такими же настройками, как у исходной учетной записи.

Нажав на кнопку *Изменить* рядом с учетной записью, вы можете изменить ее имя и/или пароль и отключить учетную запись. Отключенные учетные записи нельзя использовать для доступа к Safetica. Отключенные учетные записи можно включить снова. После включения имя пользователя и пароль остаются прежними.

Учетные записи можно удалить, нажав на кнопку *Удалить* рядом с учетной записью.

Типы учетных записей

Типы учетных записей определяют функции и настройки, к которым пользователь будет иметь доступ:

- *Администратор* — имеет эксклюзивный доступ ко всем функциям и настройкам.
- *Менеджер* — может отображать записи по всем функциям, но не может изменять настройки.
- *Настраиваемый* — вы можете установить доступ к разным функциям и настройкам в разделе настроек доступа.

Настройка доступа

Вы можете настроить следующие права доступа для каждой учетной записи. Права доступа к отдельным функциям будут применяться только к пользователям, группам или компьютерам, выбранным в дереве.

Примечание. Некоторые функции не могут быть настроены для отдельных элементов дерева. Их настройки применяются ко всей системе Safetica.

- *Не задано* — все настройки наследуются от родительского уровня.
- *Запретить все* — просмотр записей и настроек или политик установки и обновления ограничен.
- *Просмотр настроек* — право на отображение текущих настроек отдельных модулей и функций.
- *Просмотр настроек* — право отображать графику для выбранных пользователей.
- *Полный доступ* — право на отображение и изменение настроек отдельных модулей и функций.

Каждую настройку можно применить к выбранной учетной записи и отдельным модулям и функциям с разбивкой, отраженной в главном меню:

Модули:
- *Discovery*
- *Protection*

Немодульные функции:
- *Управление и настройки*
- *Другие настройки*

Любые изменения в настройках учетной записи необходимо сохранять. Для создания учетной записи рекомендуется следующая процедура: установить предварительное подключение к серверу, а затем создать для него все необходимые учетные записи. На любой другой консоли вы будете подключаться к серверу с помощью созданной учетной записи пользователя.

SIEM/Syslog

Здесь вы можете добавить адрес своего SIEM сервера или сервера системных журналов, на который будут отправляться записи о действиях, выполненных пользователями в Safetica Management Console (например, в какой раздел они получили доступ, какие настройки изменили и др.). Функция доступна только в Safetica Enterprise.

Визуализация

В журнале доступа Safetica хранятся записи о том, какой пользователь Safetica выполнил действие и когда или с каким пользователем в дереве пользователей оно было связано.

Каждая запись содержит несколько типов информации, представленной в формате столбцов:

- *Дата и время* — дата и время создания записи.
- *ПК* — имя компьютера, с которого пользователь Safetica подключился к серверу Safetica.
- *Пользователь* — имя пользователя Safetica, выполнившего действие.
- *Действие* — действие, выполненное пользователем Safetica.
- *Функция* — название экрана (функции), где выполнено действие.
- *Объект* — имя пользователя, группы или компьютера из дерева пользователей, с которым связано выполненное действие.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.4.4.9. Менеджер лицензий

Для ввода и проверки лицензий используется Менеджер лицензий. Лицензии приобретаются для клиента Safetica и назначаются конкретным рабочим станциям, на которых запущен клиент. Без назначенной лицензии функции Safetica на клиентских рабочих станциях не активны.

Менеджер лицензий размещается на консоли в меню *Обслуживание -> Управление лицензиями.*

Лицензии назначаются серверу, выбранному в дереве пользователей. Чтобы применить настройки, нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  справа вверху.

Общие настройки

Введите номер лицензии или ID пользователя в текстовое окно и нажмите *Вставить*. Активация конечных рабочих станций с клиентом будет выполняться автоматически. После подключения к серверу клиент загружает лицензию и активирует ее функции.

Расширенные настройки

В этом разделе приводится обзор добавленных лицензий. Из соображений безопасности в лицензии

отображаются только первые пять символов. Кроме того, для каждой лицензии указано, сколько она может активировать конечных рабочих станций с клиентом, а также срок действия лицензии.

Нажмите *Синхронизировать с сервером лицензий*, чтобы синхронизировать и обновить введенные вами данные лицензии с сервером лицензий Safetica.

В этот список вы можете добавить группы из дерева пользователей, для которых вы хотите изменить правила назначения лицензии. Для указанных групп вы можете разрешить или ограничить автоматическое назначение для компьютеров в группе для каждого типа лицензии.

Вы можете ввести правила автоматического назначения лицензии, нажав на *Редактировать присвоение лицензии*. Вы можете приоритезировать группы пользователей или блокировать присвоение лицензии. Если у вас меньше лицензий, чем рабочих станций с клиентом Safetica, вы можете убедиться, что лицензия присвоена приоритетным пользователям.

Группы выбираются из дерева, отображаемого после нажатия кнопки *Добавить*. Выбранные группы затем можно увидеть в списке, где вы можете включить или отключить назначение отдельных типов лицензий для Консоли управления. Правила лицензирования применяются в зависимости от их положения в списке.

В нижнем разделе представлен обзор активированных лицензий на конечных точках. Активированная лицензия на компьютере с клиентом обозначена пиктограммой  . Число в корневом элементе, который представляет сервер, обозначает общее количество активированных лицензий.

Истечение срока действия лицензии

По истечении срока действия лицензии функции Safetica на конечных рабочих станциях будут отключены. Чтобы восстановить эти функции, необходимо ввести номер новой лицензии.

Превышения лимита доступных лицензий для клиента

Если количество терминалов с клиентом, которое может быть активировано с использованием введенной лицензии, превысит разрешенное значение, на экране отобразится предупреждение о превышении лимита активированных лицензий. В этом случае вы должны приобрести лицензию, которая увеличивает количество конечных рабочих станций с клиентом.

4.4.4.10. Категории

Safetica содержит готовые категории веб-сайтов, приложений и расширений. Категории используются в разных функциях Safetica для удобства ориентации в записанных данных и настройки разных политик DLP.

В таблице категорий можно обновлять базу данных категорий, редактировать имеющиеся и создавать свои собственные категории приложений или веб-сайтов.

Настройки категорий доступны в меню *Обслуживание -> Категории*.

Описание экрана

В верхней части экрана есть кнопка *Очистить локальный кэш*. Она очищает локальный кэш с информацией о распределении приложений и веб-сайтов по категориям на всех рабочих станциях, где установлен клиент. Это действие ускоряет распространение новых данных о категориях приложений и/или веб-сайтов, измененных через консоль. Мы рекомендуем использовать эту опцию только в исключительных случаях.

Примечание. Удаление кэша категорий будет выполняться только на тех клиентах, которые подключены к серверу и управляются через запущенную консоль. Время выполнения операции зависит от того, когда отдельные клиенты загрузят актуальные настройки.

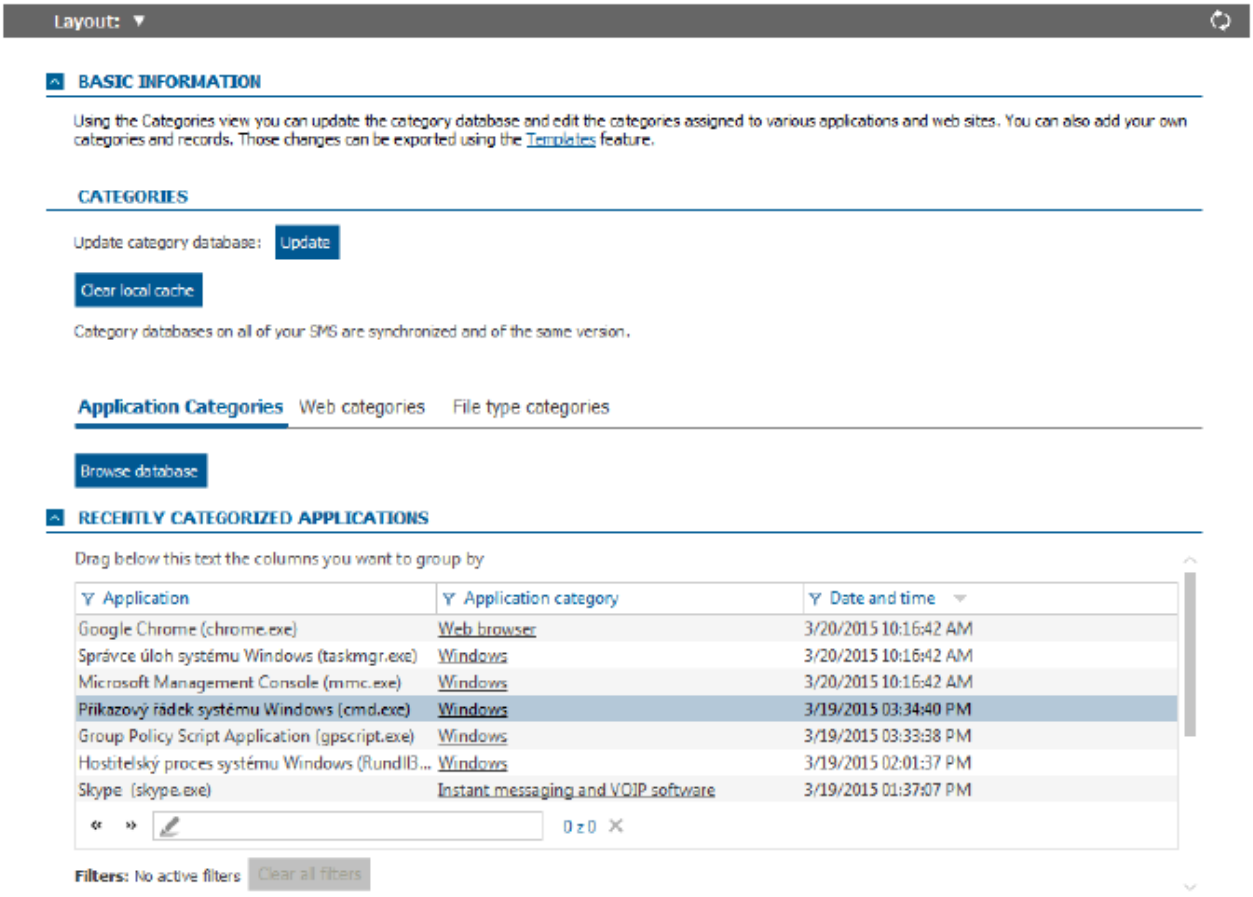
В центральной части этого экрана представлены следующие настройки для каждой категории:

- *Веб-категории* — доступ к управлению категориями веб-сайтов. Здесь вы можете добавлять свои категории и веб-сайты.
- *Категории приложений* — доступ к управлению категориями приложений. Здесь вы можете добавлять свои категории и приложения.
- *Категории файлов* — доступ к управлению категориями расширений. Здесь вы можете добавлять свои категории и расширения.

Выберите из дерева серверов тот, на котором вы хотите управлять категориями. Вы можете отобразить категории, нажав на кнопку Просмотр базы данных. Если вы отметите несколько экземпляров в дереве, после нажатия кнопки будут отображаться только те категории, которые сделаны общими для выбранных серверов.

В нижней части находится таблица со списком последних категоризированных веб-сайтов или приложений в соответствии с выбранной вкладкой. Можно вручную изменить категорию, нажав на категорию в каждой записи.

Примечание. Также вы можете использовать категоризацию в WebSafetica.



4.4.4.11. Использование компьютеров

В этом разделе вы найдете записи об активности конечных рабочих станций, на которых установлена система Safetica.

Активность пользователей может отображаться на консоли в меню *Обслуживание -> Активность пользователей (Computer utilization)*

Активность пользователей будет отображаться только для пользователей, групп, компьютеров или серверов, выбранных в дереве пользователей.

Примечание. Записи об активности на рабочем месте отправляются на сервер при выключении компьютера пользователя. По этой причине они недоступны сразу после записи.

Просмотр описания

Данные, которые которые вы видите в режиме визуализации, будут отображаться только для пользователей, ПК и групп, которые были отмечены в дереве пользователей. Экран разделен на несколько секций.

В верхней части экрана отображаются диаграммы. Вы можете найти диаграммы, доступные для текущей функции, в списке в правой части экрана. Чтобы отобразить их, нажмите и перетащите их в зону диаграмм. Диаграммы можно вернуть обратно в список, нажав на кнопку в правом верхнем углу каждой диаграммы.

Доступные диаграммы:

- *Наиболее неактивные ПК.* Эта диаграмма показывает компьютеры (до шести штук), которые используются меньше всего. Порядок компьютеров в диаграмме соответствует времени бездействия.
- *Наименее используемые ПК.* Эта диаграмма показывает компьютеры (до шести штук), которые используются меньше всего. Порядок компьютеров в диаграмме отражает бездействие, выраженное в процентах.
- *Наиболее часто используемые ПК.* Эта диаграмма показывает компьютеры (до шести штук), которые используются больше всего. Порядок компьютеров в диаграмме отражает активность, выраженную в процентах.
- *ПК с самым наибольшим временем работы.* На этой диаграмме показаны компьютеры (до шести штук), которые включены и работают дольше других.
- *Наиболее активные ПК*. Эта диаграмма показывает компьютеры (до шести штук), которые демонстрируют самую высокую активность. Порядок компьютеров в диаграмме соответствует времени активности.
- *ПК с наименьшим временем работы*. На этой диаграмме показаны компьютеры (до шести штук), которые включены и работают реже других.

Примечание. Активное время — время, которое пользователь действительно работал за компьютером. Это время определяется на основании частоты набора с клавиатуры и движения мыши.

В средней части окна визуализации отображается таблица с записями о действиях пользователей на конечной станции. Эти записи содержат следующую информацию:

- *Дата и время* — дата и время создания записи.
- *ПК* — имя компьютера, на котором была создана запись.
- *Имя пользователя* — имя пользователя, под учетной записью которого была сделана запись.
- *Действие* — тип записываемого действия:
  - *Компьютер включен* — запуск компьютера.
  - *Выключение компьютера* — выключение компьютера.
  - *Вход пользователя* — аутентификация пользователя.
  - *Выйти из системы* — выход пользователя из учетной записи.

- *Заблокировать* — блокировка компьютера.
- *Разблокировать* — разблокировка компьютера.
- *Неактивность компьютера* — пользователь не работал за компьютером.
- *Конец простоя компьютера* — время, в которое пользователь возобновил работу за компьютером.
- *Сон*
- *Пробуждение*

- *Удаленный клиент* — имя компьютера, подключенного к терминальному серверу.
- *Продолжительность* — длительность периода от начала до завершения действия (например, от запуска до выключения компьютера, от входа до выхода пользователя, от начала до завершения периода неактивности, от блокировки до разблокировки).

Внизу вы найдете обзор использования компьютера. Таблица содержит записи с информацией о том, как использовались компьютеры с установленным клиентом.

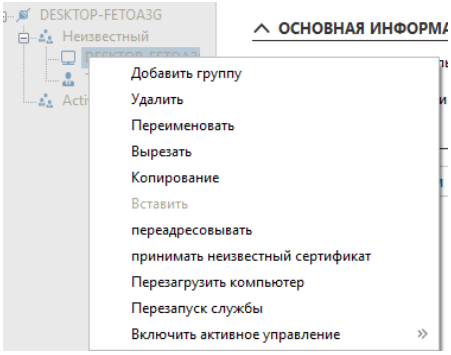
- *ПК* — имя компьютера, на котором была создана запись.
- *Общее время работы* — суммарное время работы компьютера.
- *Общая неактивность* — время, в течение которого компьютер не использовался.
- *Коэффициент использования* — использование ПК для любых действий, в процентах (период, когда пользователь работает за компьютером).

4.4.4.12. Переадресация клиента на другой сервер

Иногда по разным причинам (замена сервера, обновление, изменение в архитектуре сети) может случаться так, что существующий сервер будет недоступен для клиента Safetica по прежнему адресу. Перед внесением такого изменения существующий клиент может быть перенаправлен на другой сервер и адрес.

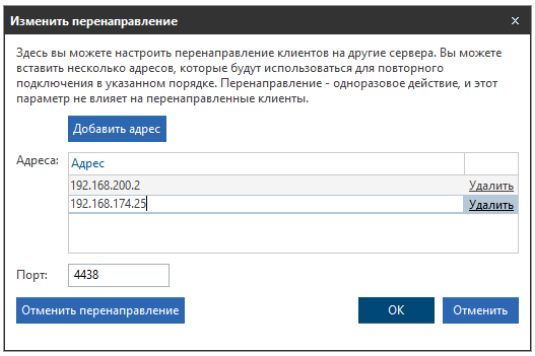
Вы можете поменять адрес сервера для разных клиентов следующим образом:

1. Отметьте те компьютеры в дереве пользователей, для которых вы хотите ввести новый адрес сервера.



2. Щелкните по ним правой кнопкой и выберите *Переадресовывать*. Откроется диалоговое окно переадресации.
3. С помощью кнопки *Добавить адрес* введите новые адреса серверов в список. Клиент всегда подключается к первому доступному серверу. Попытки подключения будут выполняться по порядку

адресов, начиная с первого в списке и до последнего. Введите порт, который клиент использует для подключения к серверу, под списком адресов. Если вы не меняете порт, оставьте порт по умолчанию. Этот порт используется для всех серверов в списке. Если вы хотите подключиться к определенному серверу через другой порт, добавьте его непосредственно после адреса сервера, отделив двоеточием (например, 192.168.200.12:4000). Подтвердите действие кнопкой *ОК*.



4. После подтверждения рядом с переадресованными компьютерами на консоли появится красная стрелка. После обновления настроек клиент подключится к новому экземпляру сервера. Если переадресация выполнена успешно, красная стрелка рядом с компьютером станет зеленой. После загрузки нового адреса клиент будет недоступен через оригинальный сервер. Администрирование перенаправленных SEC выполняется через новый сервер.

Вы можете отменить переадресацию до того, как клиент загрузит новые адреса, щелкнув правой кнопкой на опции *Отменить переадресацию*.

Переадресация клиента представляется в дереве пользователей следующий образом:

-  — была настроена переадресация.
-  — переадресация выполнена.

4.4.4.13. Защита от неавторизованных действий с клиентом Safetica

Поскольку клиент Safetica отвечает за соблюдение политики вашей организации на конечных станциях, он должен быть защищен от несанкционированного вмешательства пользователей, которые стремятся, например, обмануть блокировку или мониторинг, отключив клиент. Клиент также защищен от вмешательства пользователя с правами администратора.

Удаление, обновление или отключение клиентской службы можно настроить с консоли, или же выполнить непосредственно на конечной станции с помощью команд и пароля, сгенерированного на консоли.

Что защищено?

- *Реестр*. Невозможно изменить записи в реестрах о клиенте, в том числе IP-адрес сервера.
- *Процессы*. Защищены все процессы клиента. Их невозможно остановить. Также можно скрыть процессы в настройках клиента, чтобы список процессов не отображался.
- *Служба (STCService)* — невозможно отключить службу STCService даже с правами администратора. •
- *Установочный файл.* Невозможно переместить или переименовать файлы и папки в установочной папке клиента.
- *Файлы базы данных.* Эти файлы нельзя переместить, переименовать или удалить. Содержимое баз данных зашифровано.

- *Деинсталляция.* Клиент защищен от деинсталляции.
- *Теги.* Символы файлов (теги) защищены от перезаписи или изменения.

Разрешение на удаление и обновление с консоли

В настройках клиента каждого модуля разшерение можно предоставить, установив флажок *Удалить* или *Обновить* в дереве пользователей для выбранных пользователей, групп, конечных точек или изменив пароль для локального администрирования (см. ниже). Установка и сохранение флажка разрешает выполнение этих задач на конечных точках.

Разрешение на удаление, обновление и отключение клиентской службы с рабочей станции

Разрешение для этих задач также может быть предоставлено напрямую с конечной станции, на которой установлен клиент. Сначала вы должны сгенерировать пароль для выбранных пользователей на консоли *Настройки клиента -> Разрешенные действия.*

Для всех пользователей по умолчанию устанавливается следующий пароль: *S@fetic@2004*

Можно назначить пароль в Настройки клиента, нажав *Password (Пароль).* Вас попросят ввести новый пароль.

Выполните следующие действия:

1. Запустите командную строку от имени администратора.
2. Перейдите в установочную папку клиента. Стандартный путь: C:\Program Files\Safetica\
3. Затем введите в командную строку следующие команды, в зависимости от вашей задачи. После ввода команд вас попросят ввести пароль, который вы сгенерировали на консоли.

   Чтобы разрешить отключения службы (STCService), выполните следующую команду:

   STCService -allow stop

   Эта команда разрешает останавливать службу STCService запуском файла StopClientService.bat или включать ее запуском файла RestartClientService.bat. Это невозможно сделать без разрешения!

   Разрешить удаление клиента: *STCService -allow uninstall*

   Разрешить обновление клиента: *STCService -allow reinstall*

   ВНИМАНИЕ! Эти команды не выполняют задачи, они только дают разрешение на их выполнение.
4. После запуска перечисленных выше команд новые разрешения будут действовать до запуска команды отмены: STCService - deny. Эта команда отменит все разрешения, предоставленные вами с помощью описанных ранее команд. Эта операция не требует пароля.

4.4.5. Профиль

В этом разделе содержится основная информация о настройках вашей учетной записи, с которой вы подключаетесь к серверу.

Войдите в свой профиль, выбрав *Консоль -> Профиль.*

Учетные записи для подключения к серверу можно создать в меню *Консоль -> Обслуживание -> Управление доступом*. Там же осуществляется управление ими.

Информация о пользователе

Здесь отображается имя пользователя, под которым вы подключаетесь к серверу. Вы можете изменить пароль для этой учетной записи или выйти. После выхода из системы открывается диалоговое окно для входа на сервер.

Здесь также можно изменить язык консоли. Используйте ползунок, чтобы изменить отображаемый формат времени на разных экранах консоли. Вы можете выбрать один из двух типов форматов времени:

- *На основании выбранного языка консоли*.
- *На основании настроек системы, на которой работает консоль.*

Подключение

В этом разделе содержится информация о сервере, на который вы входите с учетной записью.

Подключение к серверу

Для подключения к новому серверу нажмите *Добавить сервер.* В диалоговом окне введите адрес сервера и порт для подключения консоли (по умолчанию это порт 4441) и подтвердите данные.

Внимание! Войти одновременно на несколько серверов вы можете только в том случае, если все подключенные серверы имеют одни и те же имя пользователя и пароль.

Редактирование настроек сервера

Вы можете изменить основные настройки подключенного сервера, нажав на соответствующую кнопку на конкретном сервере. Здесь вы сможете настроить подключение к базе данных, имя SMTP, синхронизацию с AD и другие параметры, которые подробно описаны в разделе *Настройки сервера*.

Сервер, на который вы зашли, может быть удален щелчком по ссылке на данный сервер.

Локальные настройки

В этом разделе вы найдете основную информацию о консоли, например, наименование производителя, веб-сайт и номер выпуска.

Вы можете воспользоваться ползунком, чтобы указать, следует ли запускать консоль после запуска системы.

Ползунок *Использовать прокси-сервер* позволяет указать, должна ли консоль использовать прокси-сервер для обновлений. Параметры прокси-сервера копируются из настроек Windows для текущего пользователя, от имени которого запущена консоль.

Подтвердите изменения с помощью  .

4.4.5.1. Настройки сервера

Здесь вы можете управлять базовыми настройками соответствующего сервера Safetica. Управление подключением к серверу происходит в разделе консоли Профиль.

Все изменения должны быть сохранены с помощью кнопки  в правом верхнем углу экрана.

Версия и имя

Здесь вы можете просмотреть номер версии сервера или имя сервера, которое отображается в дереве пользователей.

Настройки подключения к базе данных

Здесь вы можете настроить подключение к центральным базам данных сервера Safetica и клиента Safetica.

Примечание. Если вы указали прямой доступ к набору баз данных для клиентов Safetica в разделе Настройки клиента, сам сервер и каждый из клиентов должны иметь доступ хотя бы к одному адресу из списка баз данных. Если подключение настроено через сервер, база данных должна быть доступна только с сервера.

Нажав на кнопку *Добавить*, вы можете добавить адреса сервера MS SQL в *адреса серверов*. Сюда входят адреса, по которым базы данных Safetica будут доступны с рабочей станции и сервера. Клиент и сервер будут проверять адреса один за другим, пока не будет успешно установлено соединение с базой данных. Вы можете нажать *Удалить,* чтобы удалить адрес из списка.

В середине раздела вы найдете настройки для подключения к базам данных MS SQL.

- *Имя пользователя* — имя пользователя, которое используется для доступа к базе данных с сервера.

  Примечание. Пользователь сервера Microsoft SQL должен настроить режим аутентификации SQL (SQL Server Authentication) *и/или смешанный режим (*Mixed mode *). В экземпляре Microsoft SQL Server также должен быть разрешен этот тип аутентификации.*

- *Пароль* — пароль пользователя, который используется для доступа к базе данных с сервера.

- *Пользователь имеет самые высокие привилегии.* Используйте полосу прокрутки, чтобы указать, имеет ли вышеупомянутая учетная запись самые высокие права доступа к базе данных (*sysadmin*). Некоторые функции Safetica использовать нельзя, если учетная запись не имеет самых высоких прав:

  - Та же учетная запись, что и для подключения к серверу, будет использоваться для подключения клиента к центральной базе данных без набора самых высоких прав.
  - Кроме того, будет недоступно подключение архива в управлении базой данных.
  - Если учетная запись базы данных не имеет привилегий самого высокого уровня, то необходима роль не ниже *db-creator* для того, чтобы Safetica могла создавать свои базы данных. Если учетная запись не имеет этой роли, на SQL-сервере должны быть созданы и настроены пустые базы данных. Имена этих баз данных должны соответствовать имени базы данных, введенному в расширенных настройках (см. ниже *Префикс имени базы данных*).

  Если используется учетная запись с самыми высокими правами, в целях повышения безопасности для клиента будет автоматически создана учетная запись с ограниченным доступом к центральной базе данных.

Вы можете проверить правильность введенных данных и убедиться, что сервер успешно подключился к MS SQL, нажав *Тест соединения*.

Расширенные настройки

В расширенных настройках подключения к базе данных вы можете указать следующие параметры:

- *Имя экземпляра* — имя экземпляра сервера MS SQL. Если вы не введете имя, будет использоваться имя MSSQLSERVER.

- *Порт* — номер порта, на котором запущен экземпляр MS SQL. По умолчанию это порт 1433. Если порт не указан, будет использоваться динамический порт.
- *Префикс имен базы данных* — префикс для имен всех баз данных Safetica. Например, при вводе префикса *st* имена баз данных будут следующими: *st_main, st_data, st_category*. Если оставить поле пустым, *будет использоваться префикс safetica.*
- *Пароль учетной записи клиента* — пароль для учетной записи, используемой клиентом для доступа к базе данных. Если для подключения к центральной базе данных сервер использует учетную запись пользователя с самыми высокими правами (*sysadmin*), в базе данных будет автоматически создана учетная запись с более низкими правами. Клиент будет использовать эту учетную запись для подключения к центральной базе данных. В этом случае вы можете сбросить пароль для этой учетной записи. Для этого нажмите *Сбросить пароль.* При сбросе пароля будет автоматически сгенерирован новый пароль, после чего он будет отправлен всем SEC, подключенным к серверу. SEC будут использовать эту новую учетную запись для подключения к центральной базе данных Safetica.

Внимание! Некоторые элементы в базе данных настроек синхронизируются с базой данных записей. В частности, это относится к следующим элементам:

- *Дерево пользователей*
- *Пользователи Safetica*
- *Список внешних устройств*
- *Категории данных*

Если вы удалите любой из указанных выше элементов из настроек базы данных, будет также удалена и соответствующая информация из базы данных записей.

Примеры:

- *Если вы удалите пользователя в дереве пользователей, все связанные с ним записи будут удалены из базы данных записей.*
- *Если вы замените всю базу данных настроек новой (пустой) базой данных, все записи будут удалены из базы данных записей.*

Мы настоятельно рекомендуем создавать резервные копии в Базы данных перед каждой операцией с настройками базы данных или записями базы данных.

Active Directory

В этом разделе вы можете конфигурировать доступ к вашей Active Directory, от которой вы можете импортировать узлы, группы безопасности или отделы. Таким образом, вы можете работать с вашей существующей организационной структурой.

Введите имя пользователя и пароль Active Directory в соответствующие текстовые поля.

Чтобы импортировать части Active Directory в настроенный сервер, нажмите *Добавить*. У вас есть три варианта импорта:

- *Узел AD* — импортируйте выбранные узлы из Active Directory на настроенный сервер. После подтверждения диалога все пользователи домена и компьютеры с этих узлов будут загружены в дерево пользователей Safetica. И пользователи, и компьютеры помещаются в группу синхронизации Active Directory, из которой вы можете копировать их в другие группы.
- *Группа безопасности* — если у вас есть группы безопасности, определенные в Active Directory, вы можете выбрать, какие из них импортировать в дерево пользователей Safetica.

- *Отдел* — если в Active Directory определены отделы, вы можете выбрать, какие из них импортировать в дерево пользователей Safetica.

Используйте кнопку *Синхронизировать сейчас*, чтобы принудительно обновить пользователей и компьютеры в дереве пользователей данными из Active Directory.

Корневой сертификат

Safetica интегрируется с сетевыми коммуникациями для обнаружения или ограничения активности пользователей в сети. По умолчанию Safetica использует свои собственные сертификаты SSL, которые обеспечивают базовый уровень безопасности, используя 256-битное шифрование AES. Вы можете использовать свои собственные SSL-сертификаты чтобы еще больше повысить безопасность.

Здесь вы можете импортировать свой собственный корневой сертификат SSL. Если сертификат SSL уже используется, сначала нажмите *Удалить* и затем *Импортировать новый сертификат*.

Более подробная информация о создании собственных корневых сертификатов доступна в базе знаний.

Детальное описание использования сертификатов можно найти по ссылке.

В разделе *Alerts* можно настроить предупреждения об окончании срока действия сертификата.

Исходящий (SMTP) сервер

Здесь вы можете настроить сервер исходящей почты (сервер SMTP), который используется для отправки электронных сообщений — отчетов и предупреждений.

Вы можете проверить правильность введенных данных и корректность подключения к SMTP-серверу, нажав *Тест соединенения.* Тестовое сообщение будет отправлено с сервера на указанный адрес.

Настройка прокси-сервера

Используйте ползунок, чтобы указать, должен ли использоваться прокси-сервер.

Используйте кнопку *Скопировать системные настройки прокси*, чтобы скопировать настройки прокси-сервера из параметров Windows для пользователя, под которым запущена консоль.

Также вы можете ввести адрес прокси-сервера и порт вручную.

Анализ данных

Интеграция с инструментами аналитики доступна в Safetica Enterprise. Более подробная информация – в базе знаний.

Другие настройки

В этом разделе можно настроить уровень подробностей для журналов отладки — Ошибки, Отладка и Подробный. Только для системных администраторов и службы технической поддержки Safetica. Запуск может существенно повлиять на производительность компьютера с установленным клиентом.

4.5. Safetica Discovery

Safetica Discovery обеспечивает обзор потенциальных проблем безопасности и позволяет лучше понять процессы. С помощью Safetica Discovery вы можете проводить аудит конфиденциальных файлов, которые могут представлять угрозу безопасности. Информация, полученная от Safetica Discovery, поможет в реализации политик защиты от утечек. Благодаря аудиту оборудования вы можете видеть, на какие устройства передаются ваши файлы. Вы также можете видеть, как используются принтеры и какие файлы отправляются и скачиваются через сеть вашей компании.

Вы можете переключиться на Safetica Discovery, кликнув пиктограмму  в главном меню консоли. После нажатия на каждую из функций вы увидите ее визуализацию или обзор настроек (в зависимости от используемого режима).

4.5.1. Настройки функций

В этом режиме просмотра вы можете активировать отдельные функции Safetica Discovery.

Типы настроек

Вы можете использовать полосу прокрутки, чтобы указать, как должны работать функции:

- *Включено* — функция активна.
- *Наследовать* — функция не настраивается. Настройки наследуются от родительской группы.
- *Отключено* — функция не активна.

Настройки будут применяться только к пользователям, компьютерам, группам или веткам, которые вы выделили в дереве пользователей. Чтобы применить эти настройки, нужно сохранить изменения с помощью кнопки  . Также вы можете отменить изменения кнопкой  в правом верхнем углу.

Здесь вы можете настроить следующие функции:

- *Устройства* — фиксирует подключение и отключение периферийных USB-устройств хранения (флеш-дисков, внешних дисков и т. д.) к рабочей станции.
- *Печать* — мониторинг печати на рабочей станции.
- *Сетевой трафик* — эта функция используется для фиксации объема данных, отправленных или полученных на рабочей станции.
- *E-mails* — мониторинг связи по электронной почте на рабочей станции.
- *Файлы* — мониторинг работы с файлами на рабочей станции.

После включения функции и нажатия кнопки *Показать* дополнительные настройки некоторые дополнительные настройки, которые вы можете установить, будут отображаться в разделах *Печать* и *Файлы*.

Расширенные настройки функции печати

Если вы включите эту функцию, печать будет регистрироваться для всех приложений (включая неизвестные,

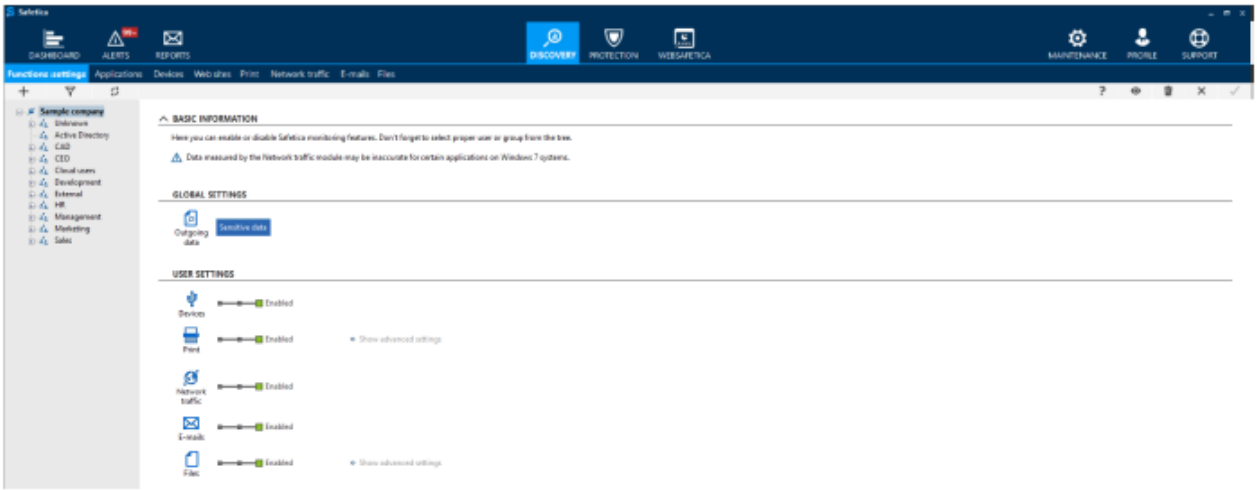
которые не интегрированы). Эти записи будут перечислены в разделе *Неизвестное приложение* в журналах аудита. Вы можете выбрать, какие приложения интегрированы (и контролируются Safetica) в разделе *Обслуживание -> Настройки интеграции -> Режим интеграции*. По умолчанию Safetica интегрируется только в известные и проверенные приложения, чтобы избежать проблем с производительностью и совместимостью.

Расширенные настройки функции файлов

Эта функция отслеживает события, которые могут привести к тому, что файлы покинут компьютер и сеть компании (например, веб-загрузка, операции с файлами на внешних устройствах или локальных путях, передача по FTP и др.). В расширенных настройках, нажав на кнопку *Добавить расширение*, вы можете включить ведение журнала операций для определенных расширений файлов. Вы можете выбрать целую категорию расширений, нажав пиктограмму с тремя точками. Однако это может повлиять на размер базы данных журналов и удобство использования/читаемость журналов аудита. Вы можете контролировать размер базы данных в разделе *Обслуживание -> Управление базой данных -> Обслуживание*.

Конфиденциальные данные в Safetica Discovery

Если вы приобрели Safetica Discovery, вы увидите специальную версию Настроек функций, которая заменяет функциональность, доступную в старших продуктах. Если у вас лицензия Safetica Protection или Safetica Enterprise, вы можете найти информацию о конфиденциальных данных в разделах *Конфиденциальные данные* и *Политики DLP*.



Чтобы создать категорию конфиденциальных данных:

1. Перейдите в *Discovery -> Настройки функций* и нажмите кнопку *Конфиденциальные данные*. Она позволит указать, какие данные вашей компании считаются конфиденциальными, и определить файлы, которые их содержат. Вы можете определить ключевые слова, указать встроенные словари, заранее определенные алгоритмы и регулярные выражения в файлах вашей компании.
2. Нажмите *Новая категория данных* и введите имя и описание категории.
3. Нажмите *Новое правило детектирования* и выберите из предварительно определенных алгоритмов и словарей, добавьте кастомные регулярные выражения или словари. Чтобы узнать больше об этих функциях, перейдите в раздел *Конфиденциальный контент* (параметр *Установить и запустить задачу обнаружения* доступен только в продуктах Safetica Protection и Safetica Enterprise).
4. Нажмите *ОК* и затем *Готово* в правом нижнем углу экрана.

4.5.2. Устройства

Функция *Устройства* предоставляет информацию о внешних устройствах, таких как USB флэшки, мобильные телефоны, принтеры и др. Вы можете видеть такую информацию, как ID устройства, используемые приложения, тип интерфейса или производитель.

Настройки

На вкладке *Discovery -> Настройки функций* вы можете включить или выключить эту функцию.

Визуализация

В режиме визуализации представлены следующие диаграммы:

- *Топ пользователей* — диаграмма отображает пользователей, которые больше всех работают со внешними устройствами (диаграмма отображает до семи самых активных пользователей).
- *Наиболее часто используемые типы устройств* — диаграмма отображает наиболее часто используемые типы внешних устройств.
- *Топ действий* — диаграмма отображает наиболее часто выполняемые действия с устройствами.

Каждая запись содержит следующую информацию:

- *Дата и время* — дата и время создания записи.
- *ПК* — имя компьютера, на котором была сделана запись
- *Имя пользователя* — имя пользователя, под учетной записью которого была сделана запись.
- *Описание* — подробное описание устройства.
- *Действие* — показывает, подключено или отключено устройство.
- *Дисковод* — какая буква диска была присвоена этому устройству.
- *Идентификация устройства* — номер, идентифицирующий устройство: <идентификатор производителя>-<идентификатор серии продуктов>-<серийный номер>.
- *Вендор* — идентификатор поставщика.
- *Тип устройства*
- *Тип интерфейса* — тип интерфейса: USB, Bluetooth, FireWire, IrDA, LPT, COM.
- *Приложение* — на каком приложении выполнялась задача.

Узнать больше об интерфейсе визуализации вы сможете в разделе *Режим визуализации*

4.5.3. Печать

Функция предоставляет подробный обзор принтеров компании и распечатанных документов. Вы можете видеть все распечатанные документы, число страниц, имена принтеров и типы печати (цветная или черно-белая).

Настройки

На вкладке *Discovery -> Настройки функций* вы можете включить или выключить эту функцию.

Визуализация

В режиме визуализации представлены следующие диаграммы:

- *Топ печатающих пользователей* — пользователи, наиболее активно использующих функцию печати. До 7 пользователей (отображается не более 7 пользователей).
- *Наиболее используемые принтеры* — устройства, наиболее активно использующие функцию печати. До 7 устройств (отображается не более 7 устройств).
- *Топ печатающих приложений* — приложения, наиболее часто используемые для печати. До 7 приложений (отображается не более 7 приложений).
- *Типы принтеров* — количество отпечатков в разбивке по типам принтеров. Различаются следующие типы принтеров: *Неизвестный тип принтера*, *Локальные принтеры*, *Виртуальные принтеры* (например, PDF Creator, XPS Writer и др.), *Сетевые принтеры, Переадресованные принтеры*.
- *Временная шкала монитора печати* — количество отпечатков за разные периоды времени.

Каждая запись содержит следующую информацию:

- *Дата и время* — дата и время регистрации записи.
- *ПК* — имя компьютера, на котором была сделана запись.
- *Имя пользователя — имя пользователя, под учетной записью которого была сделана запись.*
- *Приложение* — название приложения, из которого выполнялась печать.
- *Имя устройства* — имя использованного принтера.
- *Тип принтера* — различаются следующие типы принтеров: *Неизвестный тип принтера*, *Локальные принтеры*, *Виртуальные принтеры* (например, PDF Creator, XPS Writer и др.), *Сетевые принтеры*, *Переадресованные принтеры*.
- *Имя документа*
- *Размер бумаги*
- *Цвет печати*
- *Двусторонняя печать* — режим одновременной печати на обеих сторонах листа.
- *Общее количество страниц*

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.5.4. Сетевой трафик

Функция предоставляет инеформацию о загрузке и скачивании на конечных точках и статистистические данные об испольновании сети. Информация сгруппирована по приложениям и категориям приложений.

Примечание. Данные, собранные функцией Сетевой трафик, могут быть неточными для некоторых приложений в системах Windows 7.

Настройки

На вкладке *Discovery* -> *Настройки функций* вы можете включить или выключить эту функцию.

Визуализация

В режиме визуализации представлены следующие диаграммы:

- *Топ скачивающих пользователей* — пользователи, на которых приходится максимальный объем полученных данных (до 7 пользователей).
- *Топ загрузок в интернет по пользователям* — пользователи, на которых приходится максимальный объем отправленных данных (до 7 пользователей).
- *Топ загрузок по приложениям* — приложения, на которые приходится максимальный объем полученных данных.
- *Топ загрузок в сеть по приложениям* — приложения, на которые приходится максимальный объем отправленных данных.
- *Самые популярные загрузки по категориям приложений* — категории приложений, на которые приходится максимальный объем полученных данных.
- *Топ загрузок в сеть по приложениям* — категории приложений, на которые приходится максимальный объем отправленных данных.
- *График сетевого трафика* — сводную статистику по отправленным и полученным данным.

Каждая запись содержит несколько типов информации:

- *ПК* — имя компьютера, на котором была создана запись.
- *Имя пользователя* — имя пользователя, под учетной записью которого была сделана запись.
- С — время начала записи.
- *По* — время конца записи.
- *Получено/Отправлено* — если данные получались или отправлялись.
- *Приложение* — с какого приложения получались или отправлялись данные.
- *Категория приложения*
- *Объем данных* — объем полученных или отправленных данных в течение периода записи.

Внизу вы найдете обзор использования компьютера. Таблица содержит записи с информацией о том, как использовались компьютеры с установленным клиентом.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.5.5. E-mails

Функция предоставляет информацию об исходящих письма с вложениями, отправляемыми через почтовые клиенты и Exchange Online. Функция не проверяет электронную почту. Вы можете видеть прикрепленные файлы, темы, домены отправителя и другие детали. Полезно узнать, не пересылаются ли документы компании на личные адреса или конкурентам.

Для аудита почты выберите *Discovery -> E-mails*.

Настройки

На вкладке *Discovery -> Настройки функций* вы можете включить или выключить эту функцию.

Визуализация

В режиме визуализации представлены следующие диаграммы:

- *Отправлено/получено писем с вложениями* — количество отправленных и полученных электронных писем с вложениями за период времени.
- *Топ получателей - адреса электронной почты* — доля адресов, получающих максимальное количество электронных писем.
- *Топ получателей - домены* — доля доменов, получающих максимальное количество электронных писем.

Каждая запись содержит следующую информацию:

- *Дата и время — дата и время создания записи.*
- *ПК — имя компьютера, на котором была сделана запись*.
- *От* — адрес электронной почты отправителя. Если адрес отправителя установить не удается, это поле остается пустым.
- *Получатель* — адрес электронной почты получателя. Если адрес получателя установить не удается, это поле остается пустым.
- *Тема* — тема зафиксированного письма.
- *Файлы* — имена файлов для обнаруженных вложений.
- *Отправитель – Домен* — домен адреса электронной почты отправителя.
- *Получатель – Домен* — домен адреса электронной почты получателя.
- *Приложение* — название клиента электронной почты.
- *Размер* — размер сообщения.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.5.6. Файлы

Эта функция позволяет фиксировать информацию о файловых операциях, таких как веб-загрузка, скачивание, копирование/перемещение/переименование/создание/удаление/открытие, передачу по FTP или мессенджеры. Может быть полезно видеть, что файлы копируются на USB флэшки, загружаются на файлообменники или сообщения электронной почты.

Вы можете также включить ведение журнала операция для определенных расширений файлов.

Примечание. Отслеживание файлов, загруженных из интернета, поддерживается только для браузеров Mozilla Firefox, Internet Explorer и Google Chrome. Файлы, полученные через другие браузеры, будут зарегистрированы как новые созданные файлы.

Вы можете найти эту функцию в *Discovery -> Files*.

Настройки

На вкладке *Discovery* -> *Настройки функций* вы можете включить или выключить эту функцию.

Визуализация

В режиме визуализации представлены следующие диаграммы:

- *Наиболее активные пользователи* — список пользователей, которые активнее других работают с файлами (до 7 пользователей).
- *Наиболее активные приложения* — список приложений, которые чаще других применяются для работы с файлами.
- *Временная шкала файловых операций* — список самых распространенных файловых операций.
- *Топ операций* — количество выполненных операций и их долю от общего числа.

Каждая запись содержит несколько типов информации, представленной в формате столбцов:

- *С* — начальная дата, то есть дата первой созданной записи. Это значение зависит от параметра Обслуживание -> *Настройки клиента -> Настройки уровня агрегации журналов*.
- По — конечная дата, то есть дата последней созданной записи Это зависит от параметра *Обслуживание - > Настройки клиента -> Настройки уровня агрегации журналов*.
- *ПК — имя компьютера, на котором была сделана запись*.
- *Имя пользователя* — имя пользователя, под учетной записью которого выполнялась операция.
- *Приложение* — название приложения, которое выполняло файловую операцию.
- *Источник* — имя и расположение файла, к которому применялась файловая операция.
- *Место назначения* — адрес местоположения, в которое копируются или перемещаются файлы.
- *Тип источника* — различаются следующие типы:
  - Локальный путь
  - USB-носитель
  - Сетевой путь
  - FTP
  - CD/DVD
  - Прочие внешние носители
  - Удаленная передача (передача файлов с использованием службы удаленного рабочего стола Microsoft или TeamViewer)
  - Облачный диск (локальная папка, подключенная к облачному хранилищу). Поддерживаются следующие поставщики облачных дисков: *Google Drive, OneDrive, Dropbox, Box sync*.
  - Интернет
  - E-mail
  - Webmail
  - Мгновенный обмен сообщениями (мессенджеры)
  - Файлообменники
  - Мобильные устройства
- *Тип назначения* — различаются следующие типы:
  - Локальный путь
  - USB-носитель
  - Сетевой путь
  - FTP
  - CD/DVD

- Прочие внешние носители
- Удаленная передача (передача файлов с использованием службы удаленного рабочего стола Microsoft или TeamViewer)
- Облачный диск (локальная папка, подключенная к облачному хранилищу). Поддерживаются следующие поставщики облачных дисков: Google Drive, OneDrive, Dropbox, Box sync.
- Интернет
- E-mail
- Webmail
- Мгновенный обмен сообщениями (мессенджеры)
- Файлообменники
- Мобильные устройства

- *Операция* — тип выполняемой файловой операции: *Открытие, Копирование, Удаление, Перемещение, Создание, Загрузка из интернета, Передача по FTP, Переименование, Веб-загрузка, Отправка в мессенджере, E-mail.*
- *Исходное устройство* — имя и идентификатор SID. Щелкнув по имени устройства, вы получите подробную информацию о нем. Здесь можно указать, к каким зонам должно принадлежать это устройство. Для этого нажмите кнопку *Редактировать зону* и отметьте нужные зоны.
- *Устройство назначения* — имя и идентификатор SID. Щелкнув по имени устройства, вы получите подробную информацию о нем. Здесь можно указать, к каким зонам должно принадлежать это устройство. Для этого нажмите кнопку *Редактировать зону* и отметьте нужные зоны.
- Файл — имя файла. Если вы создаете группу, упорядочение или фильтр на основе этого столбца, имя файла извлекается из столбца *Источник*. Если сведения об источнике отсутствуют, имя файла извлекается из столбца *Адрес назначения*.
- *Размер файла*
- *Расширение* — расширение файла. Если вы создаете группу, упорядочение или фильтр на основе этого столбца, расширение файла извлекается из столбца *Источник*. Если сведения об источнике отсутствуют, расширение файла извлекается из столбца *Место назначения*.
- *Конфиденциальный контент* — содержит ли файл конфиденциальные данные.
- Риск – информирует, можно ли считать операцию потенциальной угрозой безопасности. Более подробная информация о рисках – в базе знаний.
- Действие
- Категория данных – категории, которыми отмечен файл.
- Детали

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.6. Safetica Protection

Раздел Protection доступен только в продуктах Safetica Protection и Safetica Enterprise. Здесь вы можете защитить конфиденциальные данные компании от недопустимого использования, чтобы предовратить финансовые потери и ущерб для репутации. В сочетании с Safetica Discovery, Safetica Protection информирует вас и защищает от вредоносной активности, которая может привести к утечке данных.

Есть несколько способов настроить DLP защиту в разделе Protection:

- *На основании содержания (Конфиденциальные данные)* — основной и самый простой метод

использует глубокий анализ содержимого данных. Это наша рекомендуемая форма защиты DLP. Конфиденциальные данные идентифицируются на основе контента с использованием словарей, алгоритмов, ключевых слов или регулярных выражений. Данные никак не помечаются.

- *Отслеживание данных сторонними приложениями (Существующая классификация(метаданные))* — еще один вариант защиты DLP основанный на существующих метках метаданных, выполненных, например, другим приложением классификации. Этот подход может быть использован для защиты данных, которые уже были классифицированны сторонними приложениями (например, как внутренние, конфиденциальные и т. д.).
- *На основе контекста (Контекстные правила*) — защита DLP на основе контекста работы с данными. Это означает, что данные защищены в зависимости от того, кто работает с данными, где они хранятся, где данные перемещаются, в каких приложениях и т.д. Конфиденциальные данные защищены меткой Safetica. Этот метод может использоваться для защиты данных, которые не могут быть классифицированы по содержанию. Это сложнее реализовать и поддерживать. Метод требует более глубоких знаний о Safetica, а также детального анализа и соотвествия корпоративым процессам по работе с данными.
- *На основе свойств файлов (Свойства файла)* — категории данных свойств файлов позволяют защищать файлы на основе их свойств, таких как расширение, независимо от содержания или классификации. Нвапример, вы можете защитить все исходящие файлы .pdf или .cad. Эти категории могут расширять существующие политики DLP для защиты файлов, которые нельзя сканировать на предмет классификации или конфиденциальных данных (например, зашифрованных файлов).

4.6.1. Журналы DLP

Журналы DLP содержат записи об операциях с данными или приложениями, на которые распространяются политики DLP.

Журналы DLP находятся по следующему пути *Protection -> Журналы DLP*.

Доступны следующие графики:

- *Топ пользователей* — показывает пользователей, которые больше всего работают с файлами.
- *Топ действий* — показывает наиболее частые действия, выполняемые с файлами.
- *Топ операций* — показывает наиболее частые операции с файлами.
- *Наиболее активные приложения* — показывает приложения, наиболее часто используемые для работы с файлами.
- *Временная шкала файловых операций* — показывает временную шкалу файловых операций.

Каждая запись содержит несколько типов информации, представленной столбцами:

- *С* — время, когда началась запись.
- *По* — время, когда запись завершилась.
- *ПК* — название ПК, на котором была сделана запись.
- *Имя пользователя* — имя пользователя, под которым была выполнена файловая операция.
- *Приложение* — имя приложения, которое выполнило файловую операцию.
- *Источник* — имя и путь к файлу, участвующему в операции.
- *Место назначения* — путь к пункту назначения при копировании или перемещении.
- *Тип источника* — является ли исходный путь к файлу локальным, внешним или сетевым.

- *Место назначения* — является ли целевой путь к файлу локальным, внешним или сетевым.
- *Исходное устройство* — имя устройства и SID. После нажатия на название будет отображена подробная информация об устройстве. Здесь вы можете указать, к каким зонам должно принадлежать устройство. Вы можете сделать это, нажав кнопку *Изменить зону* и добавив в соответствующие зоны.
- *Целевое устройство* — имя устройства и SID. После нажатия на название будет отображена подробная информация об устройстве. Здесь вы можете указать, к каким зонам должно принадлежать устройство. Вы можете сделать это, нажав кнопку *Изменить зону* и добавив в соответствующие зоны.
- *Файл* — имя файла. Если вы создаете группу, упорядочиваете или фильтруете с помощью этого столбца, имя файла будет взято из столбца *Источник*. Если источник пуст, имя файла будет взято из столбца *Назначение*.
- *Операция* — тип выполняемой операции с файлом: открыие файла, копирование файла, перемещение файла, удаление файла, печать, снимок экрана, буфер обмена, запись на диск, E-mail, запись, чтение, создание файла.
- *Действие* — была ли операция разрешена или заблокирована Safetica.
- *Контекст действия*.
- *Категория данных* — к какой категории данных относится файл.
- *Модули* — имя модуля, который создал запись: *Журналы DLP, Защита диска или Контроль устройств.*
- *Детали*
- *Размер файла*
- *Конфидициальные данные* — была ли операция выполнена с конфиденциальными данными.
- *Безопасная зона*
- *Политика*
- Риск – информирует, можно ли считать операцию потенциальной угрозой безопасности. Более подробная информация о рисках – в базе знаний.
- Теневая копия – информирует, была ли создана теневая копия файла. Если копия создана, ее можно получить, перейдя по ссылке *Да (collect)*.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.6.2. Правила DLP

Safetica использует правила DLP для защиты данных на конечных точках и контроля поведения приложений.

Более подробная информация о правилах DLP доступна в базе знаний.

Как создать новое правило DLP

Откройте *Консоль -> DLP -> Правила DLP*

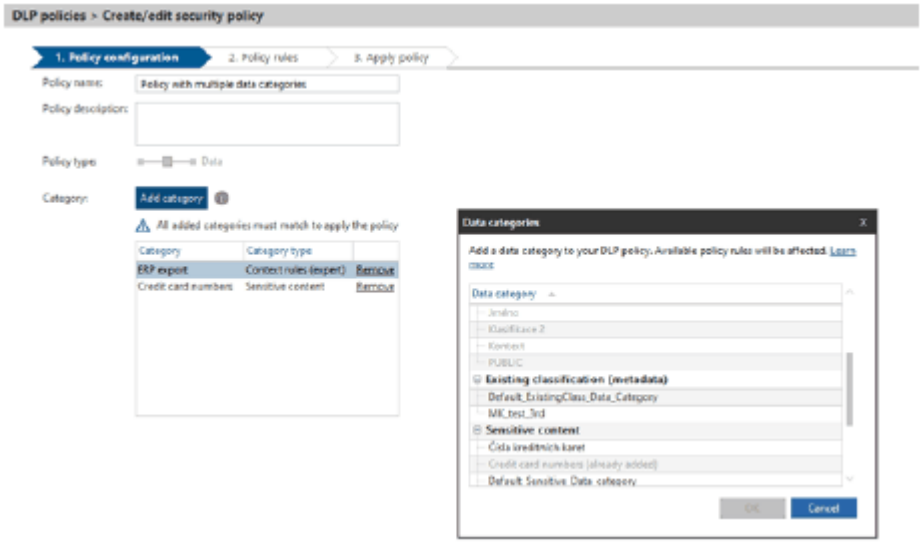
Нажмите кнопку *Новая политика*.

Конфигурация

Введите имя и описание политики в конфигурации, выберите ее тип (*Общая, Категория данных, Категория приложения*).

Для политик категорий приложений выберите категорию приложения, применимую к данной политике, нажав кнопку *Выбрать категорию*.

Для политик данных выберите категории данных, применимые к данной политике, нажав кнопку *Добавить категорию*. Вы можете включить любое число категорий данных в категории *Конфиденциальные данные* и *Существующая классификация* (метаданные) по своему усмотрению. При этом вы можете включить только одну категорию данных типа *Контекст*.



Примечание. Политики, объединяющие несколько типов категорий данных, помечены как Несколько категорий данных в списке политик DLP. Если вы выберите такую политику, то увидите определенные категории данных, которые она включает, справа в разделе Сведения о политике -> Категории.

Правила

Выберите режим и настройте правила политики DLP.

Более подробная информация о функции *Теневая копия* доступна в базе знаний.

Более подробная информация о функции *Замещение* доступна для режимов *Журнал и блокировка* в базе знаний.

Чтобы просмотреть доступные правила политики DLP, нажмите *Настроить*. Проверенные правила будут помещены в список, и вы сможете их установить. Вы также можете использовать шаблоны политик для создания новой политики DLP. Шаблоны представляют собой заранее созданные группы правил. Каждая политика создает новый шаблон, который вы сможете использовать позже при создании других политик DLP.

Применение политики

Нажмите *Добавить пользователей*. В дереве пользователей выберите пользователя или группу, для которой вы хотите применить данную политику DLP.

4.6.3. Категории данных

Здесь можно создавать неограниченное количество категорий данных. Категории данных используются для разделения файлов на разные группы в зависимости от того, кто, где и как может работать с файлами. Впоследствии для каждой категории данных можно создавать разные политики DLP.

Существует четыре типа категории данных:

- *Конфиденциальные данные* — данные идентифицируются на основе контента с использованием словарей, алгоритмов, ключевых слов или регулярных выражений.
- *Существующая классификация* — предварительно классифицированные данные, идентифицированные с использованием тегов, метаданных или меток файлов другого типа.
- *Контекстные правила* — данные, которые нельзя классифицировать по содержанию. Требует экспертных знаний и дополнительного обслуживания.
- *Параметры файлов* — файлы защищены на основе их параметров (например, расширений). Подходит для файлов, которые нельзя сканировать на предмет классификации или конфиденциального контента (например, зашифрованных файлов).

Категории данных доступны по пути *Protection -> Категории данных*

Создание новой категории данных

В левой части раздела показан список категорий данных. После выбора категории в списке ее название и описание, а также дополнительные параметры управления категорией будут отображаться справа.

Если вы хотите создать новую категорию данных, нажмите *Новая категория данных*. Введите имя и описание категории данных и выберите ее тип (*Конфидициальные данные, Существующая классификация, Контекстные правила*) и при необходимости измените дополнительные параметры.

Дополнительные параметры

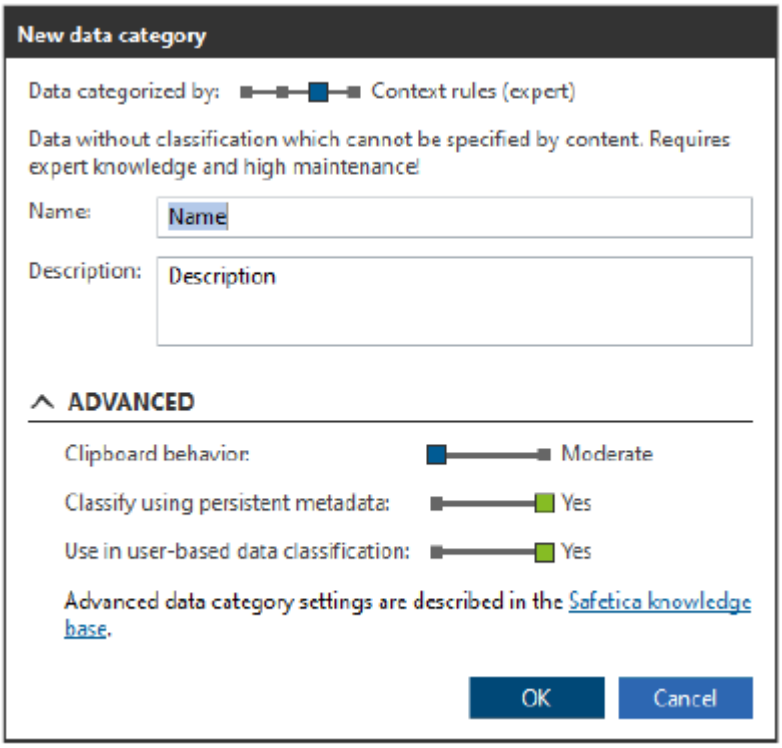
Для категорий данных *Существующая классификация* и *Контекстные правила* расширенные настройки позволяют настроить поведение буфера обмена:

- *Умеренный* — буфер обмена ограничен, только если он используется для передачи потенциально опасного контента.
- *Строгий* — буфер обмена всегда будет ограничен в соответствии с политиками DLP.

  Примечание. Строгий режим для буфера обмена может привести к неожиданному распространению категорий данных и ограничений. Подробнее – в базе знаний.

Для контекстных правил вы также можете классифицировать данные с использованием постоянных метаданных. Более подробная информация доступна в базе знаний.

Для контекстных правил, если у вас включены постоянные метаданные, вы также можете использовать категорию в классификации на основе пользователей. Узнать больше – в базе знаний.



Нажмите OK, чтобы добавить категорию в список, показанный слева. Сохраните изменения с помощью кнопки ✓. Также вы можете отменить изменения кнопкой ✕ в правом верхнем углу.

Выберите вновь созданную категорию и настройте предполагаемое поведение для типа категории справа:

- *Конфидициальные данные*
- *Существующая классификация*
- *Контекстные правила*
- *Параметры файлов*

Редактирование категории данных

Вы можете редактировать имя и описание существующей категории данных, нажав кнопку *Изменить*, расположенную рядом с каждой категорией данных в списке.

Удаление контекстных меток

Правила удаления меток позволяют удалять метки из файлов, которым эти метки были присвоены случайно (например, из-за ошибок в настройке правил). Соблюдайте крайнюю осторожность при использовании этих правил, чтобы не удалить метки из тех файлов, которые должны их иметь. Эти правила применяются независимо от выбранной категории.

Нажав на кнопку *Удаление контекстной метки*, вы откроете мастер удаления.

Создание правила удаления меток производится так же, как и создание правила расположения в *Контекстных правилах*. Единственное отличие состоит в том, что это правило удаляет метки их тех файлов, которые соответствуют его условиям. Также на втором шаге мастера вы можете выбрать, следует ли удалять все метки или только те, которые указаны в соответствующем списке.

4.6.3.1. Конфиденциальные данные

Используя правила поиска содержимого файлов, вы можете помечать файлы, содержащие конфиденциальные данные. Вы можете выбрать один из нескольких предустановленных шаблонов для поиска конфиденциального содержимого или определить свой собственный шаблон, используя ключевые слова и регулярные выражения.

Правила обнаружения

Вы можете создать несколько правил для обнаружения конфиденциального контента. Каждое правило будет применяться только при соблюдении всех условий правила. Конфиденциальные данные будут обнаружены, если применяется хотя бы одно правило обнаружения в списке правил.

Минимальное число совпадений

Введите число, соответствующее порогу обнаружения. Если в файле содержится меньше конфиденциальных данных, чем указано, файл будет проигнорирован и не будет отмечаться как конфиденциальный.

Используя правила поиска контента файлов, вы можете отмечать файлы, содержащие конфиденциальные данные. Вы можете выбрать один из нескольких предустановленных шаблонов для поиска конфиденциального контента или определить собственный шаблон, используя ключевые слова и регулярные выражения.

Предустановленный конфиденциальный контент (алгоритмы и словари)

- Номера кредитных карт
- IBAN — международный формат номеров банковских счетов
- Идентификаторы физических и юридических лиц Бразилии
- Персональные идентификаторы граждан Чехии и Словакии в стандартном формате
- Национальные идентификационные номера граждан Дании
- Национальные идентификационные номера граждан Швеции
- Польские национальные идентификационные номера (PESEL)
- Номера паспортов граждан Польши
- Идентификационные номера VAT налогоплательщиков Германии
- Идентификационные номера VAT налогоплательщиков Испании
- Национальные идентификационные номера граждан Норвегии
- Номера идентификационных карт граждан Сингапура
- Номера идентификационных карт граждан Эквадора
- Номера идентификационных карт граждан Турции
- Номера идентификационных карт граждан Польши
- Национальные номера социального страхования граждан Великобритании
- Номера социального страхования граждан Канады

- Номера социального страхования граждан США. Сюда включаются также номера ITIN (Индивидуальный номер идентификации налогоплательщиков)
- Система проверяет данные одновременно по номерам социального страхования США и по данным из словарей на основе HIPAA. К этим словарям применяются регулярные обновления определений, и в них содержится полные актуальные списки компаний, медицинских состояний и лекарственных средств

  Примечание. Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA — Health Insurance Portability and Accountability Act) регулирует правила работы с персональной информацией о состоянии здоровья пациентов в медицинских учреждениях США.

Настраиваемые выражения

В этом разделе вы можете указать собственные регулярные выражения и ключевые слова для поиска конфиденциальных данных в содержимом файла. Ключевые слова не чувствительны к регистру. Регулярные выражения оцениваются на основе синтаксиса ECMAScript. Примеры регулярных выражений можно найти в базе знаний.

Настраиваемые словари

Здесь вы можете выбрать словари, содержащие слова, которые будут определяться как конфиденциальные данные.

Нажав кнопку *Управление словарями*, вы можете удалить, импортировать или обновить существующие словари. Если вы хотите импортировать собственный словарь, создайте текстовый файл со словами, которые вы хотите определять как конфиденциальные данные. Каждое слово необходимо ставить с новой строки.

Вы можете применять созданное правило обнаружение только для выбранного типа файлов. Более подробная информация – в базе знаний.

Вы можете использовать функцию оптического распознавания символов (OCR - Optical character recognition) для поиска конфиденциальных данных в изображениях. Детали – в базе знаний.

Настройка и запуск задачи обнаружения

Вы можете разрешить системе выполнять поиск файлов, которые соответствуют выбранной категории данных. Результаты поиска отображаются в визуализации. Чтобы запустить поиск, выполните следующие действия:

1. Введите следующее:
   - Имя и описание
   - Выберите пользователей, компьютеры или группы из дерева пользователей, где вы хотите запустить поиск.

2. На втором этапе укажите, какие файлы и папки будут участвовать в поиске.

- Установите правила:
  - *Расположение* — только файлы, которые находятся или будут находиться в этих папках, и все их подпапок и соответствуют другим частям правила (расширения, ключевые слова и т.д.) будут участвовать в поиске.
  - *Расширения* — введите расширения в список или выберите категорию расширения. Файлы с расширениями, указанными в списке или содержащимися в выбранной категории расширений, будут участвовать в поиске.

- *Повторение задачи* — вы можете повторять задачу поиска через регулярные промежутки времени. Для повторных поисков вы можете указать, на каких компьютерах и для каких пользователей они будут повторяться. Это может быть необходимо, например, из-за прав доступа.

3. Файлы, к которым применяются все части правила, будут защищены. Не все части правила должны быть настроены. Достаточно ввести хотя бы одну часть. Если часть не введена, она будет применяться ко всем случаям. Нажмите *Готово*, чтобы подтвердить генерацию правила.
4. Для сохранения нажмите 

Вы можете снова запустить поиск, отредактировав и подтвердив в мастере задачи поиска, описание в четырех пунктах выше.

4.6.3.2. Существующие классификации

Если вы используете сторонние инструменты для классификации конфиденциальных данных, вы можете настроить их в этом разделе. Более подробная информация о поддерживаемых технологиях и инструкции по настройке доступны в базе знаний.

Настройка и запуск задачи обнаружения

Вы можете разрешить системе выполнять поиск файлов, которые соответствуют выбранной категории данных. Результаты поиска отображаются в визуализации. Чтобы запустить поиск, выполните следующие действия:

1. Введите следующее:
   - Имя и описание
   - Выберите пользователей, компьютеры или группы из дерева пользователей, где вы хотите запустить поиск.

2. На втором этапе укажите, какие файлы и папки будут участвовать в поиске.

- Установите правила:
  - *Расположение* — только файлы, которые находятся или будут находиться в этих папках, и все их подпапок и соответствуют другим частям правила (расширения, ключевые слова и т.д.) будут участвовать в поиске.
  - *Расширения* — введите расширения в список или выберите категорию расширения. Файлы с расширениями, указанными в списке или содержащимися в выбранной категории расширений, будут участвовать в поиске.

- *Повторение задачи* — вы можете повторять задачу поиска через регулярные промежутки времени. Для повторных поисков вы можете указать, на каких компьютерах и для каких пользователей они будут повторяться. Это может быть необходимо, например, из-за прав доступа.

3. Файлы, к которым применяются все части правила, будут защищены. Не все части правила должны быть настроены. Достаточно ввести хотя бы одну часть. Если часть не введена, она будет применяться ко всем случаям. Нажмите *Готово*, чтобы подтвердить генерацию правила.
4. Для сохранения нажмите 

Вы можете снова запустить поиск, отредактировав и подтвердив в мастере задачи поиска, описание в четырех пунктах выше.

4.6.3.3. Контекстные правила

На основе правил файлы, соответствующие им, будут помечены выбранной категорией данных или изменением тегов.

Каждому файлу может быть присвоена только одна категория данных.

Вы можете узнать больше о классификации с использованием постоянных метаданных в базе знаний.

Настройки

Для поиска и отметки файлов можно использовать несколько видов правил.

Правила приложений

Правила приложений позволяют отслеживать приложений и категории приложений, выходные файлы которых будут отмечаться меткой соответствующей категории данных.

Например, вы можете настроить такое правило, которое отмечает все файлы всех приложений из категории CAD, чтобы далее применять ко всем этим файлам определенный набор ограничений.

Чтобы создать правило приложения для выбранной категории данных, выполните следующее:

1. Выберите нужную категорию данных в списке категорий данных, затем нажмите кнопку *Добавить* в разделе *Правила приложений*. Откроется мастер создания правила приложений.
2. На первом его шаге введите следующие данные:

- Имя и описание правила.
- Режим правила:
  - *Тестирование* — метки не будут присваиваться файлам. В этом режиме создаются записи для файлов, соответствующих созданному правилу. В режиме визуализации вы можете проверить список файлов, которым будут присвоены метки. Затем вы можете изменить режим правила.
  - *Маркировка* — всем файлам, соответствующим этому правилу, присваиваются метки соответствующей категории данных.
- *Приложения* — выберите категорию приложения. Выходные файлы из приложений выбранных категорий будут отмечены метками соответствующей категории данных.
- *Расширения* — введите расширения в список или выберите категории расширений. Файлам с расширениями, указанными в списке или содержащимися в выбранной категории расширений, будет присвоена соответствующая метка.
- Дополнительно:
  - *Ключевые слова* — введите ключевые слова в списки. Файлы, содержащие хотя бы одно из заданных ключевых слов в имени файла, будут помечены. В качестве ключевого слова можно использовать даже регулярные выражения. Подробнее.
  - *Действия по маркировке*:

        - *Слияние тегов по приоритету* — файл будет помечен по категории данных, имеющей более высокий приоритет. Если файл уже помечен тегами, приоритеты текущей и новой категорий данных сравниваются, и файл маркируется категорией с более высоким приоритетом.
        - *Заменить метки* — замена существующего тега выбранной категорией данных. Приоритет категории данных игнорируется.
    - *Включая системные* — с помощью этой опции можно активировать тегирование системных файлов. В настройках интеграции можно добавить пользовательские пути к системным файлам. Используйте эту опцию с осторожностью и только в обоснованных случаях.

  Метки присваиваются файлам, которые соответствуют одновременно всем условиям правила. Не обязательно заполнять все разделы параметров правила. Достаточно указать одно любое условие. Любой незаполненный раздел применяться не будет.

3. Щелкните *Конец*, чтобы подтвердить создание правила.

Правила веб-сайтов

Правила веб-сайтов можно использовать для присвоения меток файлам, загруженным с определенных сайтов или доменов, относящихся к определенной категории веб-сайтов.

Например, такой тип правил можно использовать для присвоения меток всем файлам, загруженным из корпоративной системы CRM.

Нажав на кнопку *Добавить*, вы откроете мастер создания правил веб-сайтов.

Правила веб-сайтов создаются аналогично правилам приложений. Разница только на втором шаге, где вместо списка приложений можно настроить список веб-адресов. Метки будут применяться только к тем файлам, которые загружены из внесенных в список адресов и соответствуют всем остальным условиям правила (расширения, ключевые слова и т. п.).

Кроме того, в дополнительных настройках есть *Опция применения меток*.

- *Область применения меток* — по умолчанию метка присваивается всему веб-контенту.
    - *Только загруженные и открытые файлы* — помечаются только файлы, загруженные из интернета, и открытые файлы.
    - *Весь веб-контент* — весь контент, загруженный из интернета, будет помечен, включая контент, скопированный через буфер обмена.

Правила расположения

Правила расположения позволяют выбрать определенные папки, к содержимому которых будут применяться метки. Все файлы, сохраненные в этих папках, будут автоматически отмечены. Кроме того, вы можете настроить регулярно выполняемое правило для присвоения меток файлам в выбранных папках, в том числе помещенным в эти папки с компьютеров, на которые не распространяется защита Safetica.

Нажав на кнопку *Добавить*, вы откроете мастер создания правила расположений.

Создание правил расположений происходит точно так же, как и правил приложений. Разница есть только на втором шаге, где вместо списка приложений можно настроить список расположений. Метки будут применяться только к тем файлам, которые располагаются или будут помещены в указанные папки (включая все вложенные папки) и соответствуют всем остальным условиям правила (расширения, ключевые слова и т. п.).

Кроме того, вы можете здесь настроить задачу для регулярного присвоения файлам меток в соответствии с настроенными правилами. Благодаря этому метки будут присваиваться даже тем файлам, которые помещаются в выбранные расположения с компьютеров, на которые не распространяется защита Safetica.

Для повторяющейся задачи вы можете указать пользователя, от имени которого они будет выполняться (например, если нужны определенные права доступа).

Правила распространения меток

Правила распространения меток позволяют настроить следующую схему работы: если в приложении открыт файл с меткой выбранной категории, эта же метка будет присвоена и всем файлам, созданным в этом приложении в этот период.

Примечание. Независимо от наличия этого правила, метка всегда распространяется на все файлы, сохраненные из приложения через стандартное диалоговое окно сохранения (Сохранить как...). Правило распространения меток применяется к нестандартным методам сохранения данных из приложения. Сюда относятся, к примеру, операции преобразования форматов.

Нажав на кнопку *Добавить*, вы откроете мастер создания правила распространения меток.

Создание правила распространения меток происходит точно так же, как и правила приложений. Разница заметна лишь на втором шаге, где не нужно настраивать список приложений. Это правило применяется ко всем приложениям, в которых открываются любые файлы с метками выбранной категории. Метки распространяются только на те файлы, которые имеют расширения из указанного списка, а также соответствуют всем остальным условиям правила, таким как ключевые слова.

Повторение заданий

Вы можете выполнять задания присвоения меток через регулярные интервалы. Благодаря этому метки будут присваиваться даже тем файлам, которые помещаются в выбранные расположения с компьютеров, на которые не распространяется защита Safetica. Для повторяющегося задания вы можете указать пользователя, от имени которого они будет выполняться. Это полезно, например, если нужны определенные права доступа.

Расширенные параметры

- Операции меток:
  - *Слияние меток по приоритету* — файл будет помечен категорией данных, которая имеет более высокий приоритет. Если файл уже помечен, сравниваются приоритет текущей и новой категорий данных, а файл помечается категорией с более высоким приоритетом.
  - *Заменять метки* — заменяет существующий тег выбранной категорией данных. Приоритет категории данных игнорируется.

Метки присваиваются файлам, которые соответствуют одновременно всем условиям правила. Не обязательно заполнять все разделы параметров правила. Достаточно ввести одно любое условие. Любой незаполненный раздел применяться не будет.

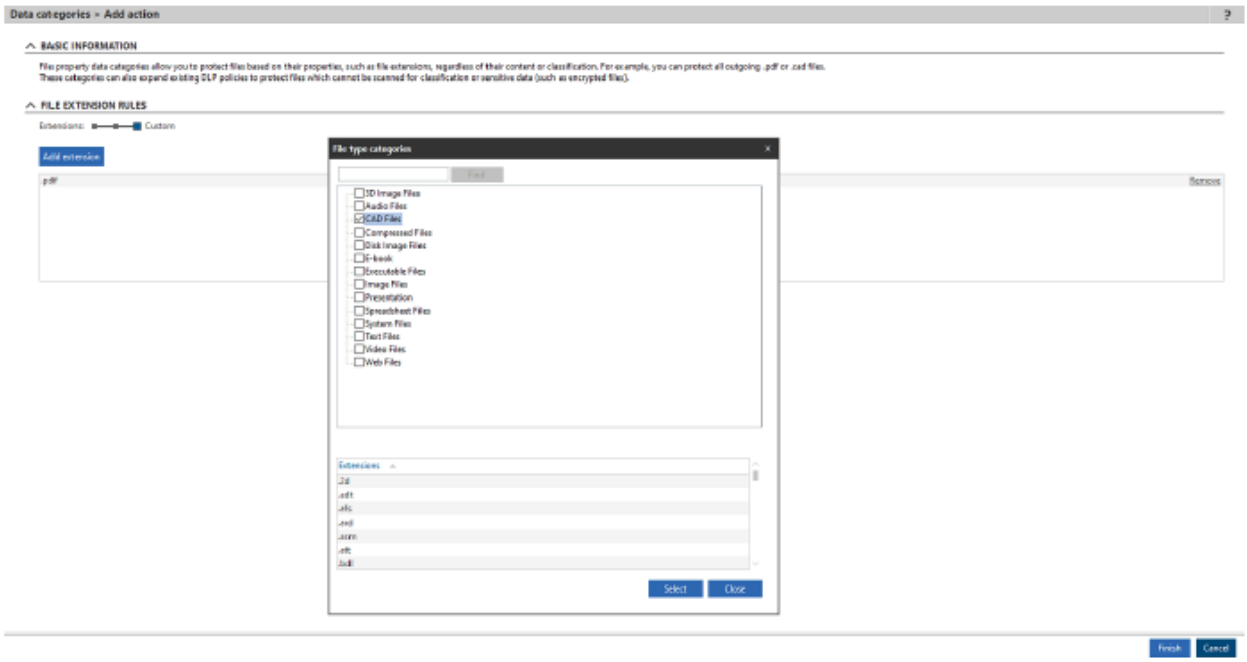
Нажмите *Конец,* чтобы подтвердить создание правила.

4.6.3.4. Свойства файла

Используя *Свойства файла*, можно защитить файлы, несовместимые с технологией сканирования контента Safetica, сторонними классификациями или выбрать защиту всех файлов с заданным расширением.

Чтобы создать категорию для заданных расширений, выполните следующее:

1. Выберите нужную категорию данных (*Safetica Management Console > Protection > Категории данных*)
2. Нажмите *Новая категория данных* и выберите *Свойства файла* с помощью ползунка *Данные по категориям*.
3. Введите имя и описание категории и нажмите *ОК*.
4. В списке категорий слева выберите вновь созданную категорию и нажмите *Настроить категорию данных*.
5. С помощью ползунка *Расширения* выберите *Пользовательский* и нажмите *Добавить расширение*.
6. Вы можете ввести свои расширения или нажать на иконку с многоточием  и выбрать категории из списка. Когда вы закончите, нажимте Выбрать.
7. Нажмите *Готово* в правом нижнем углу экрана.



4.6.4. Зоны

Зоны можно использовать для создания именованных наборов внешних устройств, принтеров, IP-адресов, сетевых путей и адресов электронной почты, на которые можно указывать ссылки как на независимые объекты. Вы можете впоследствии использовать их в правилах DLP.

Настройки

Левая часть зоны просмотра отображает список созданных зон. Выбрав зону в списке слева, вы увидите слева подробную информацию о ней: имя и описание.

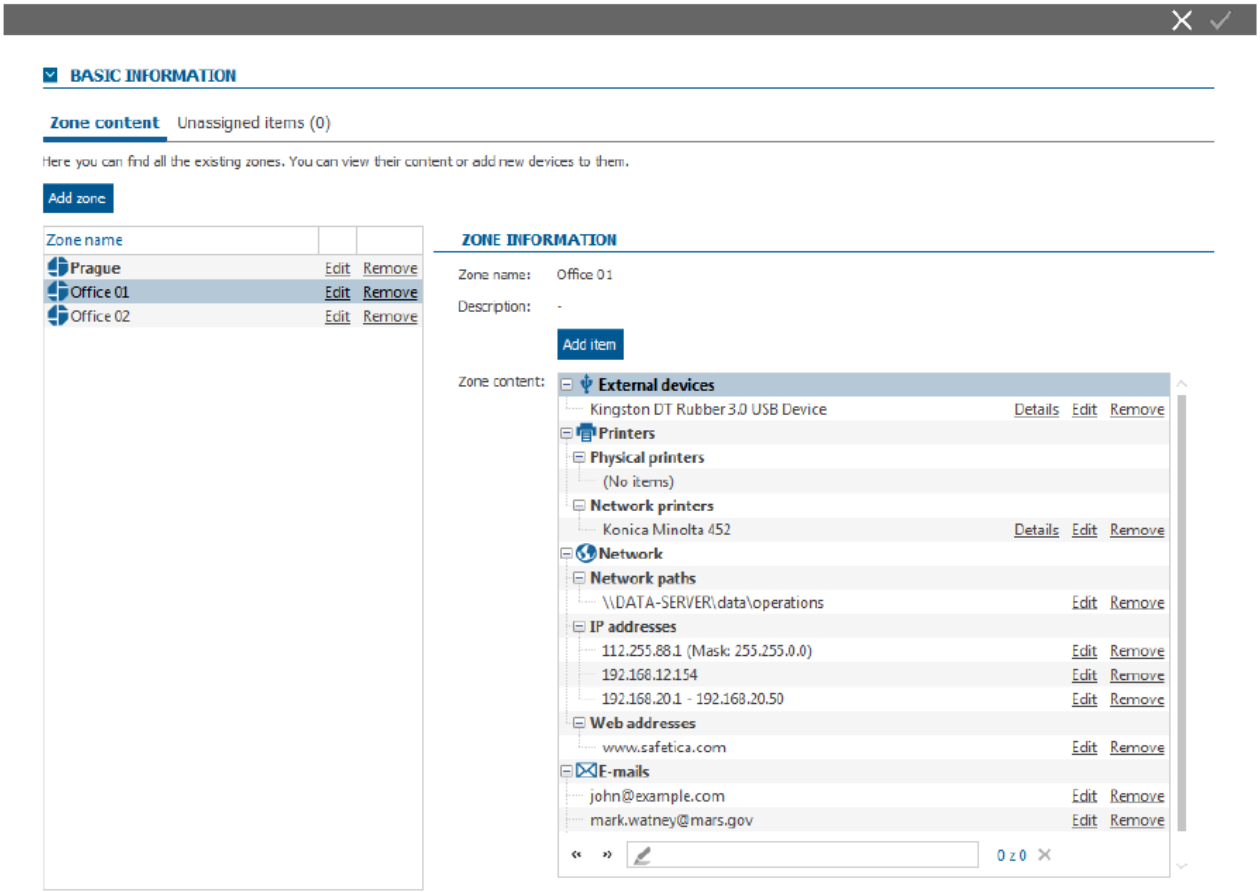
Щелкните *Добавить зону,* чтобы открыть диалоговое окно создания новой зоны, затем введите для нее имя и описание и укажите, будет ли она иметь родительскую зону. Родительскую зону можно выбрать в раскрывающемся списке.

Щелкнув *Изменить* для любой зоны в списке слева, вы можете изменить ее имя и описание.

Над списком зон можно выбрать две вкладки: *Содержимое зоны* и *Нераспределенные элементы.* Содержимое правого сегмента этого экрана зависит от выбранной слева вкладки.

- *Содержимое зоны* — нажмите *Добавить элемент* в разделе содержимого зоны, чтобы открыть мастер создания нового элемента и добавить элемент в эту зону. Также вы можете отредактировать уже существующий в зоне элемент кнопкой *Изменить*.
- *Неназначенные элементы* — в этом разделе справа отображается список доступных внешних устройств и принтеров, подключенных на рабочих станциях, где установлен клиент. Здесь отображаются только те устройства и принтеры, которые пока не назначены никакой зоне.
  - Переместив их в средний список или нажав кнопку *Добавить*, вы можете поместить эти элементы в зону, отмеченную слева.
  - Щелкните *Удалить*, чтобы вернуть устройство или принтер в группу неназначенных устройств.
  - Нажав *Изменить*, вы можете изменить описание устройства, которое будет отображаться в записях в консоли и в окне извещений на компьютере, где установлен клиент.
  - Щелкнув *Детали*, вы можете отобразить подробную информацию об элементе.

Примечание. С помощью мыши вы можете выбирать и перемещать сразу несколько элементов в списках.



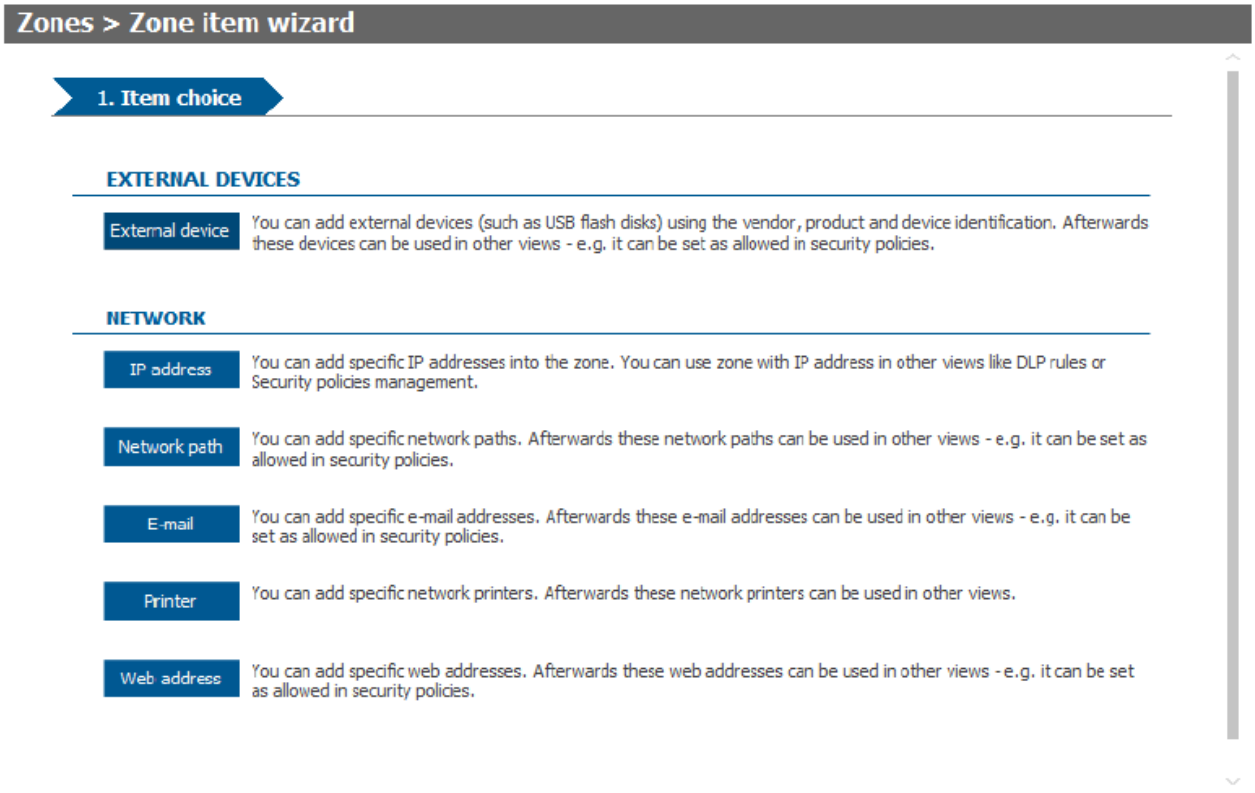
Создание новой зоны и добавление элементов в неё

Щелкните *Добавить зону,* чтобы открыть диалоговое окно создания новой зоны, затем введите для нее имя и описание.

Чтобы изменить содержимое зоны, выполните следующие действия:

1. В списке зон слева отметьте ту зону, содержимое которой вы хотите изменить. Слева внизу отобразится текущее содержимое зоны. Нажмите на ссылку R Удалить рядом с соответствующим элементом зоны, чтобы удалить его. Нажмите Добавить элемент, чтобы добавить новый элемент в зону.
2. Мастер добавления предложит вам выбрать элемент из списка допустимых для зоны:
    - *Внешние устройства*
    - *IP-адреса*
    - *Сетевые пути*
    - *Email*
    - *Принтеры*
    - *Веб-адрес*

Щелкните по элементу, который вы хотите добавить. Откроется соответствующий экран для его добавления.



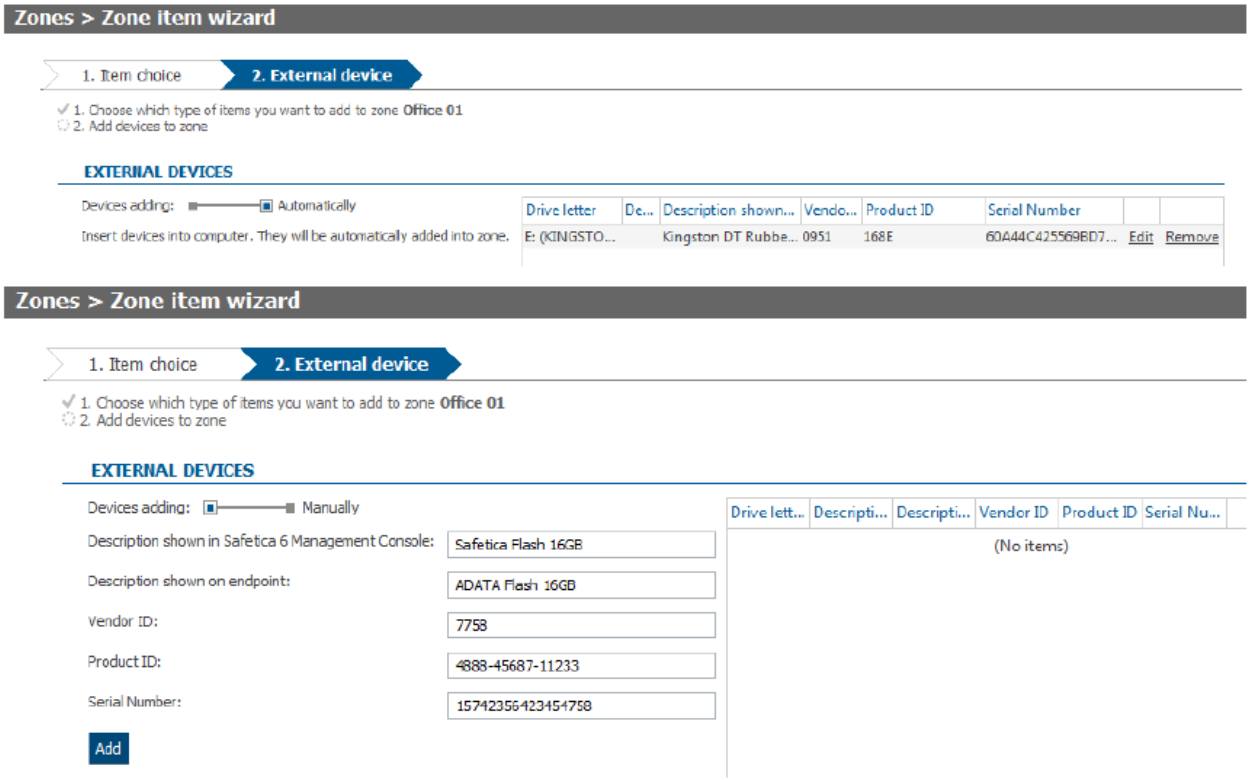
Добавление внешнего устройства

У вас есть два варианта для добавления в зону внешнего устройства. С помощью ползунка выберите один из них:

- *Автоматически* — в автоматическом режиме достаточно лишь подключить внешнее устройство хранения к компьютеру, на котором запущена консоль. Подключенное устройство сразу добавляется в список.
- *Вручную* — в этом режиме данные об устройстве нужно ввести в текстовые поля, чтобы устройство правильно обнаруживалось. Введите идентификатор поставщика, идентификатор устройства и

серийный номер. Эту информацию можно найти на упаковке устройства или узнать у производителя. Устройство добавляется в список после нажатия кнопки Добавить.

Вы можете добавить в список несколько внешних устройств.

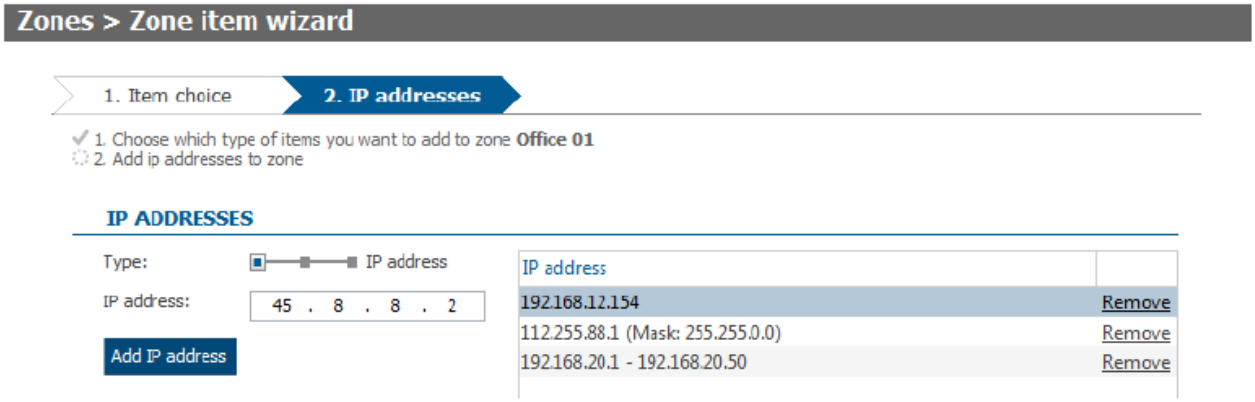


Добавление IP-адресов

У вас есть три варианта для добавления IP-адресов в зону. С помощью ползунка выберите один из них:

- *IP-адреса* — введите IP-адрес в соответствующее поле и щелкните Добавить IP-адрес, чтобы добавить один IP-адрес в список справа.
- *IP с маской* — введите IP-адрес и маску в соответствующее поле и щелкните Добавить IP-адрес, чтобы добавить IP-адрес в список справа.
- *Диапазон IP* — введите начальный и конечный адреса диапазона в соответствующее поле и щелкните Добавить IP-адрес, чтобы добавить диапазон в список справа. Теперь все добавленные адреса, включая начальный и конечный, будут считаться принадлежащими этой зоне.

Вы можете добавить в список несколько адресов.

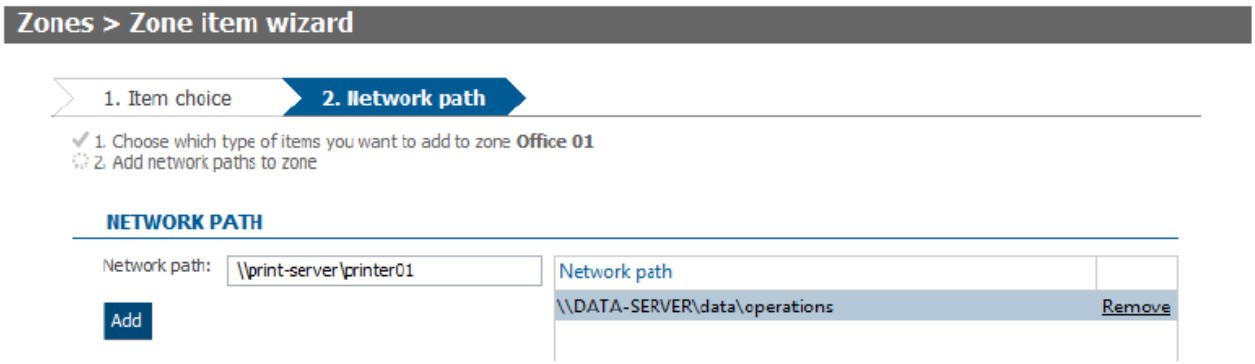


Добавление сетевого пути

Введите путь к общему файловому ресурсу в формате сетевого адреса (например, \\Data\Finance) в текстовое поле, затем щелкните Добавить, чтобы добавить этот путь в список справа.

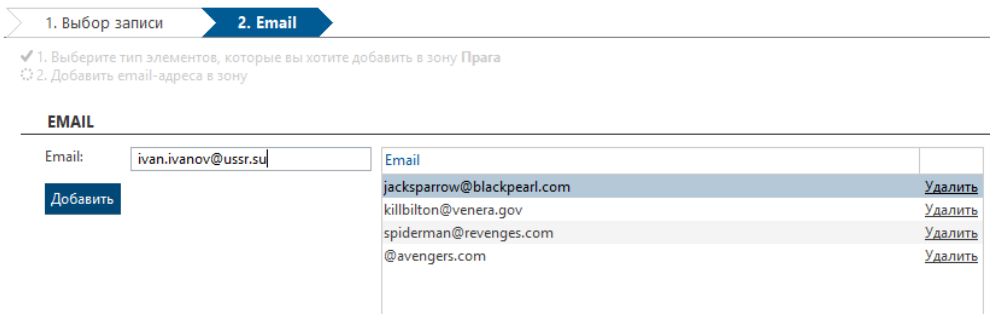
Вы можете добавить в список несколько сетевых путей.

Также вы можете добавить в зону сразу весь компьютер с несколькими общими файловыми ресурсами. Для этого введите путь к корневой папке этого компьютера. Например, так: \\DATA-SERVER\. В этом случае в зону добавляются сразу все общие файловые ресурсы выбранного компьютера.



Добавление email

Введите адрес электронной почты в соответствующее поле и щелкните *Добавить*, чтобы добавить этот адрес в список справа. Вы можете добавлять адреса двумя способами: в обычном формате (например, name@domain.com) или целыми доменами (например, @domain.com обозначает anna@domain.com, thomas@domain.com и т. д.), чтобы добавить в зону сразу все адреса электронной почты в этом домене.



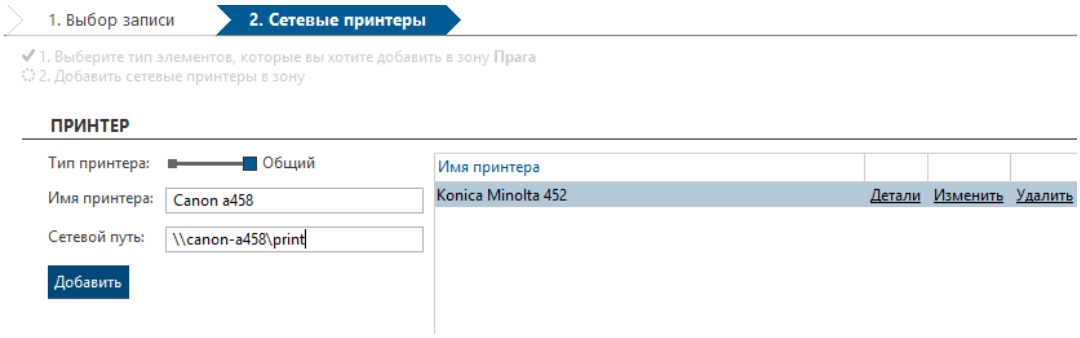
Вы можете добавить в список несколько адресов электронной почты.

Добавление принтера

Вы можете добавить в зону принтеры двух типов. С помощью ползунка выберите нужный тип принтера.

- *TCP/IP* — используется для принтеров, подключенных напрямую к сети. Введите имя и IP-адрес принтера в соответствующие поля. Затем с помощью ползунка выберите тип протокола для принтера (Raw или LPR), а затем, в зависимости от типа протокола — введите номер порта или имя очереди. Щелкните Добавить, и новый принтер сразу же отобразится в списке справа.
- *Общий принтер* — используется для принтеров, доступ к которым предоставляется через компьютер. Введите имя принтера и путь к нему в соответствующие поля (например, \\Server\SharingName). Щелкните Добавить, и новый принтер сразу же отобразится в списке справа.

Вы можете добавить в список несколько принтеров.

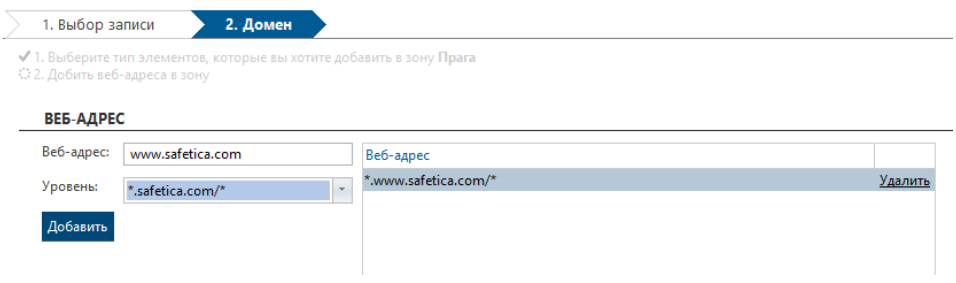


Адреса веб-сайтов

Вы можете добавить в зону адреса веб-сайтов. Для каждого добавленного адреса можно отдельно указать уровень применения правила. Например, если вы введете адрес www.facebook.com,, вы можете выбирать из следующих вариантов для параметра Уровень:

- *www.facebook.com/** — так вы включите в зону сам адрес www.facebook.com и любые другие адреса, начинающиеся с этой строки. Например, www.facebook.com/AAA/, www.facebook.com/AAA/BBB, и т. д.
- **.www.facebook.com/** — так вы включите в зону сам адрес www.facebook.com и любые другие адреса, содержащие эту строку. Например, www.facebook.com/AAA/, ccc.www.facebook.com/AAA/BBB и т. д.
- **.facebook.com/** — так вы включите в зону все адреса, содержащие подстроку .facebook.com. Например, www.facebook.com/AAA/, ccc.facebook.com/AAA/BBB и т. д.
- **.com/** — так вы включите в зону все адреса, содержащие подстроку .com. Это действие блокирует все веб-сайты, чей адрес заканчивается на .com. Например, www.facebook.com/AAA/ или www.cnn.com.

По умолчанию используется первый вариант, то есть www.facebook.com/*.



3. Завершив ввод информации, щелкните Готово, чтобы добавить элемент в зону. Для подтверждения изменений нажмите кнопку  в правой верхней части.

4.6.5. Защита диска

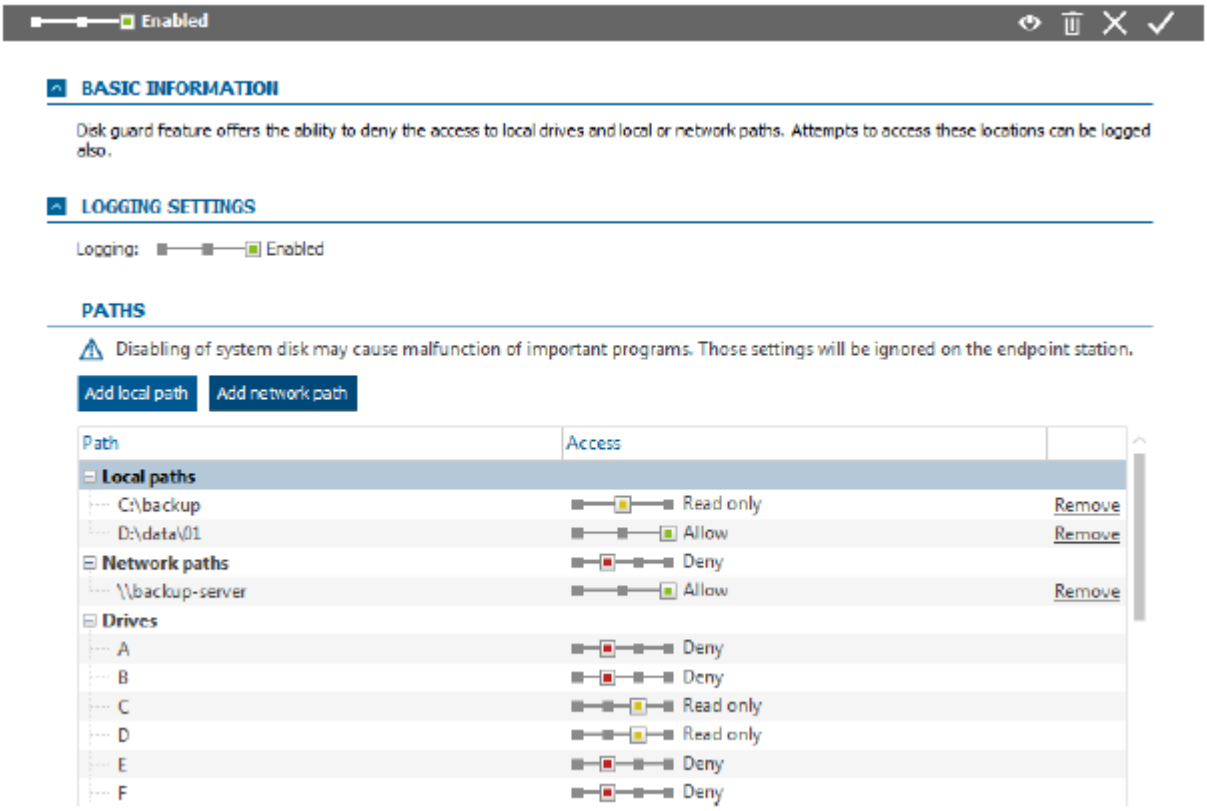
Защита диска позволяет настроить права доступа для пользователей, компьютеров или групп при обращении к системным или сетевым путям или сетевым дискам, используя простой набор правил. Например, вы можете выбрать диски, к которым у пользователей будет доступ только для чтения, а также выбрать конкретные пути или папки.

Защита диска включается следующим образом: *Protection -> Защита диска*

Настройки

В режиме настроек консоли эта функция может быть включена или отключена с помощью ползунка в заголовке этого экрана.

С помощью ползунке *Логирование* вы можете включить регистрацию действий доступа. Записи об этих действиях можно просмотреть в режиме визуализации.



Правила путей

Вы можете настроить права доступа для путей трех типов:

- *Локальные пути* — обозначающие папки на самой рабочей станции (например, D:\Folder\name).

- *Сетевые пути* — обозначающие папки, предоставленные в совместный сетевой доступ. Эти пути нужно вводить в формате сетевого адреса (например, //Shared/Folder).
- *Диски* — здесь указывается список букв, обозначающих диски. Для каждого отдельного диска можно настроить права доступа.
- *Облачные хранилища* — здесь вы можете указать настройки доступа к локальным папкам, для которых настроена синхронизация с поддерживаемой облачной службой. Поддерживаются следующие облачные службы: *OneDrive Personal, OneDrive Business, SharePoint, Google Drive, Dropbox* и *Box Sync*. Вы можете настроить права доступа сразу для всех поддерживаемых служб или для каждой из них отдельно.

  Примечание. Для каждой отдельной облачной службы в таблице указано количество выбранных в дереве компьютеров, на которых установлен соответствующий облачный клиент.

Здесь доступны следующие варианты настройки доступа:

- *Наследовать* — функция не настраивается. Настройки наследуются от группы более высокого уровня.
- *Запретить* — у пользователей нет доступа к дискам или путям.
- *Только чтение* — пользователь может только посматривать и читать данные на этом диске или по этому пути. Он не сможет сохранить данные на этот диск или в этот путь.
- *Разрешить* — этот диск или этот путь доступен пользователю для для любых операций.

Вы можете добавить локальный путь с помощью кнопку *Добавить локальный путь*.

Вы можете добавить сетевой путь с помощью кнопку *Добавить сетевой путь*.

Вы можете настроить права доступа для конкретных дисков (обозначенных буквами) в разделе Диски.

Примечание. Если вы введете в качестве параметра букву системного диска, на рабочей станции могут заблокироваться функции операционной системы.

Визуализация

В режиме визуализации представлены следующие диаграммы:

- *Топ пользователей* — содержит список пользователей, для которых существует больше всего записей (до 7 пользователей).
- *Наиболее активные приложения* — содержит список приложений, которые пользователи чаще всего используют для работы с файлами (до 7 приложений).
- *Топ операций* — список самых распространенных файловых операций.
- *Временная шкала файловых операций* — содержит распределение количества файловых операций по времени.

Каждая запись содержит несколько типов информации, представленной в формате столбцов:

- *Дата и время* — дата и время регистрации записи.
- *ПК* — имя компьютера, на котором была сделана запись.
- *Имя пользователя* — имя пользователя, под учетной записью которого была сделана запись.

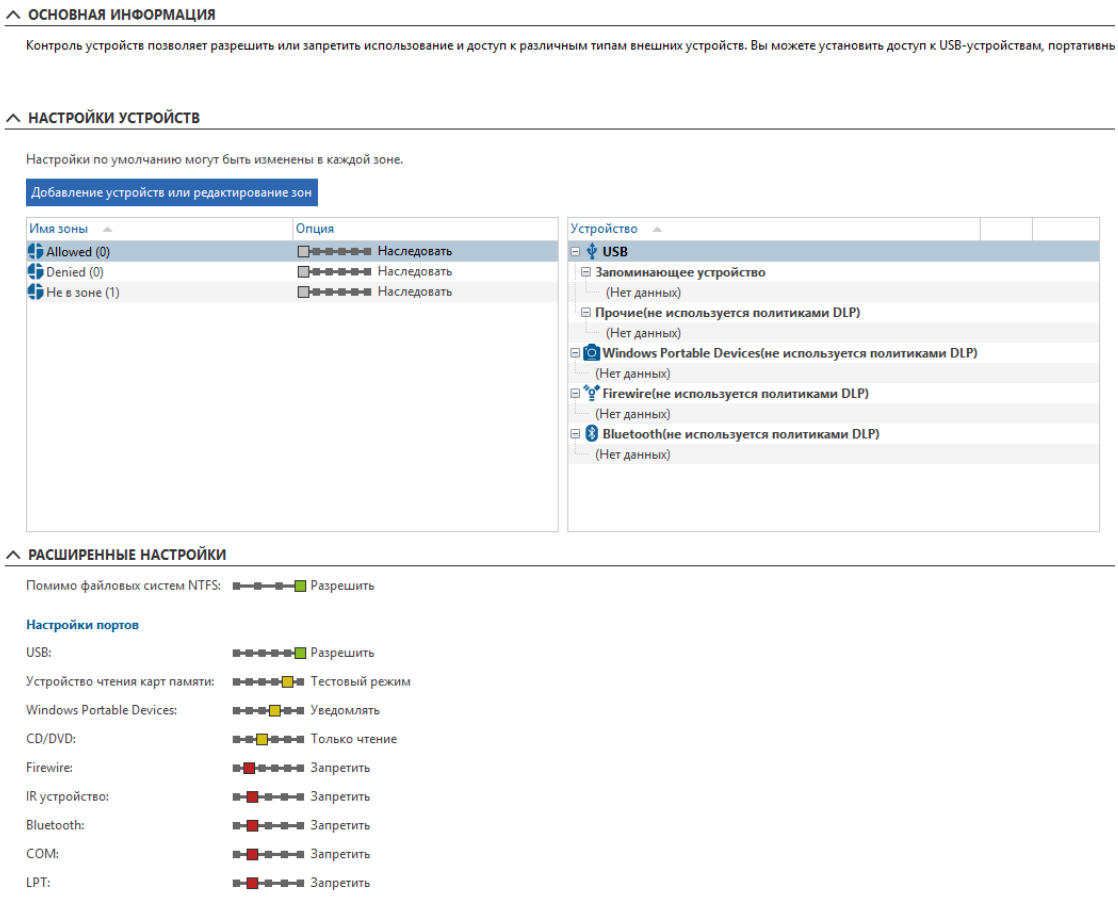
- *Приложение* — название приложения, которое использовало путь доступа или диск.
- *Источник* — имя и расположение файла, к которому применялась операция.
- *Место назначения* — целевое расположение для операций копирования и перемещения.
- *Операция* — тип выполненной операции доступа: *Открыть файл, Удаление файла, Перемещение файл, Записать, Читать.*
- *Действие* — название выполненного действия: *Запретить, Тестовый, Уведомлять, Отключить, Шифровать*
- *Тип источника* — тип исходного пути к файлу: *Локальный путь, Сетевой путь, USB, FTP, CD/ DVD, Другие внешние, Web, Облачный диск, Удаленная передача.*
- *Исходное устройство* — название исходного устройства.
- *Тип адресата* — тип пути назначения для файла: *Локальный путь, Сетевой путь, USB, FTP, CD/ DVD, Другие внешние, Web, Облачный диск, Удаленная передача.*
- *Устройство назначения* — название целевого устройства.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.6.6. Контроль устройств

Функция управления устройствами позволяет включить или отключить использование внешних устройств разных типов и/или доступ к ним. Доступ к устройствам USB, Bluetooth, FireWire и переносным устройствам под управлением ОС Windows можно регулировать через функцию Зоны.

В режиме настройки консоли вы можете отключить или включить эту функцию, используя полосу прокрутки в заголовке экрана.



Настройки устройств

В этом разделе вы можете подробно настроить основные параметры управления устройствами.

- *Настройки устройств по умолчанию* — здесь вы можете указать, какие параметры управления устройствами будут изначально применяться для новых внешних устройств. Функция настройки устройств позволяет выбрать следующие варианты в качестве настройки по умолчанию:
    - *Наследовать* — настройки наследуются от родительской группы.
    - *Запретить* — чтение и запись на внешних устройствах запрещены.
    - *Только чтение* — для внешнего устройства допускается только чтение, но не запись.
    - *Уведомлять* — при использовании внешнего устройства пользователь увидит уведомление в диалоговом окне, при этом будет создана соответствующая запись.
    - *Тестовый режим* — действует так же, как и предыдущий вариант *Уведомлять*, но пользователь не получает никаких предупреждений. Создается только запись регистрации. Этот режим предназначен для тестирования настроек.
    - *Разрешить* — чтение и запись на внешних устройствах разрешены.

Эти настройки будут применяться ко всем внешним устройствам, для которых они не были изменены отдельно.

В настройках по умолчанию можно указать список зон и список устройств в этих зонах. Для каждой зоны, включенной в таблицу, вы можете настроить права доступа к внешним устройствам этой зоны. Все параметры

здесь те же, что и для настройки по умолчанию.

Примечание. Можно использовать вложенные зоны. Настройки, указанные для зоны нижнего уровня, имеют более высокий приоритет, чем для ее родительской зоны.

Щелкните кнопку *Добавление устройств или редактирование зон,* чтобы перейти к режиму Зона. Здесь вы можете быстро создать новые зоны или изменить содержимое уже имеющихся. Каждая зона может содержать внешние устройства следующих типов:

Расширенные настройки

В этом разделе вы можете более подробно указать глобальные настройки для доступа к устройствам конкретных типов или к файловым системам, отличным от NTFS. Например: FAT32, ext3, ext4 и т. д.

Для других файловых систем можно выбрать следующие режимы доступа:

- *Наследовать* — настройки наследуются от родительской группы.
- *Запретить* — доступ к устройствам с файловой системой, отличной от NTFS, будет отключен.
- *Только чтение* — доступ к устройствам с файловой системой, отличной от NTFS, только для чтения.
- *Разрешить* — доступ к устройствам с файловой системой, отличной от NTFS, будет включен.

Примечание. Этот параметр имеет наиболее высокий приоритет в этом режиме просмотра.

Для каждого типа внешних устройств (порта) можно настроить параметры, указанные в настройках по умолчанию: *Наследовать, Запретить, Только чтение, Уведомлять, Test Тестовый режим, Разрешить.*

Типы устройств (портов):

- *USB-носитель*
- *Устройство чтения карт*
- *Windows Portable Devices*
- *CD / DVD*
- *FireWire*
- *IrDA*
- *Bluetooth*
- *COM*
- *LPT*

Примечание. Настройки портов имеют более низкий приоритет, чем настройки зон. Например, если USB-порты отключены в настройках портов, но отдельно включены для конкретной зоны, то в этой зоне использование USB-портов будет разрешено.

Визуализация

Сохраняются записи обо всех операциях доступа к устройствам, определенным в режиме настроек. В режиме визуализации представлены следующие диаграммы:

- *Топ пользователей* — содержит список пользователей, для которых существует больше всего записей.

- *Топ действий* — доля выполненных действий с внешними устройствами.
- *Наиболее часто используемые типы устройств* — доли типов используемых устройств.
- *Лучшие политики безопасности* — наиболее часто применяемые политики безопасности.
- *Топ заблокированных пользователей* — пользователи, для которых чаще всего применялась блокировка.

Каждая запись содержит несколько типов информации, представленной в формате столбцов:

- *Дата и время* — дата и время регистрации записи.
- *ПК* — имя компьютера, на котором была сделана запись.
- *Имя пользователя* — имя пользователя, под учетной записью которого была сделана запись.
- *Тип устройства*
- *Описание* — подробное описание устройства. Щелкнув по описанию устройства, вы увидите подробную информацию о нем. Здесь можно указать, к каким зонам должно принадлежать это устройство. Для этого нажмите кнопку *Редактировать зону* и отметьте нужные зоны.
- *Действие* — указывает, что устройство было Подключено, Отключеннный, Носитель подключен, Доступно для чтения, Записать.
- *Дисковод* — какая буква диска была присвоена этому устройству.
- *Идентификация устройства* — идентификаторы имеют следующий формат: <идентификатор производителя>-<идентификатор продукта>-<серийный номер>.
- *Вендор* — наименование поставщика устройства, включая идентификатор.
- *Политика безопасности* — указывает, какая политика безопасности была применена для этого действия.
- *Приложение* — указывает, в каком приложении выполнялось действие.
- *Причина ограничения* — какой режим ограничений применялся для отказа в доступе к внешнему устройству: порт, устройство, файловая система, не удалось разблокировать с помощью BitLocker.
- *Тип интерфейса* — тип внешнего устройства, а именно: *USB, Bluetooth, FireWire, IrDA, LPT, COM*.

Узнать больше об интерфейсе визуализации вы сможете в главе *Режим визуализации*.

4.6.7. Устройства BitLocker

Эта функция позволяет применить к USB-дискам шифрование BitLocker. Вы можете предоставить доступ к зашифрованным устройствам конкретным пользователям, компьютерам или группам.

Шифрование устройств

Вы можете настроить шифрование USB-дисков, подключенных к компьютеру, на котором установлены консоль или клиент.

Примечание. Компьютер, на котором выполняется консоль и будет применяться шифрование, должен поддерживать функцию BitLocker (Windows 7 Ultimate, Enterprise, Windows 8.1 Pro и выше, Windows 10 Pro и

выше, Windows Server 2008 R2 и выше).

Вы можете добавить в список устройств BitLocker внешние устройства из зон, нажав на кнопку *Добавить*.

Вы можете удалить устройство из списка с помощью кнопки *Удалить*.

Шифрование на конечной точке, где установлен клиент

1. Перейдите на вкладку *Protection -> Устройства Bitlocker*.
2. Назначьте флеш-накопитель пользователю, компьютеру или группе.
3. Выберите *Шифровать* для флеш-накопителя с помощью ползунка в колонке *Действие*.
4. Теперь флеш-накопитель будет шифроваться при подключении к компьютеру, которому он назначен.

Шифрование на компьютере, где установлена консоль

1. Откройте консоль с правами администратора.
2. Подключите флеш-накопитель к компьютеру, на котором работает консоль.
3. Перейдите на вкладку *Protection -> Устройства Bitlocker*.
4. Выберите *Шифровать* для флеш-накопителя с помощью ползунка в колонке *Действие*. Флеш-накопитель будет зашифрован.

Назначение доступа

Выполните назначение с помощью ползунка *Назначить* в таблице со списком устройств. Доступ к зашифрованным флеш-накопителям предоставляется только пользователям, группам и компьютерам, выделенным в дереве пользователей.

Доступ к зашифрованому флеш-накопителю

На компьютерах, которым назначено устройство хранения, флеш-накопитель автоматически разблокируется (предоставляется для доступа) сразу после подключения. На компьютерах, которым не назначен флеш-накопитель или на которых не установлен клиент, для доступа к этому флеш-накопителю необходимо ввести пароль.

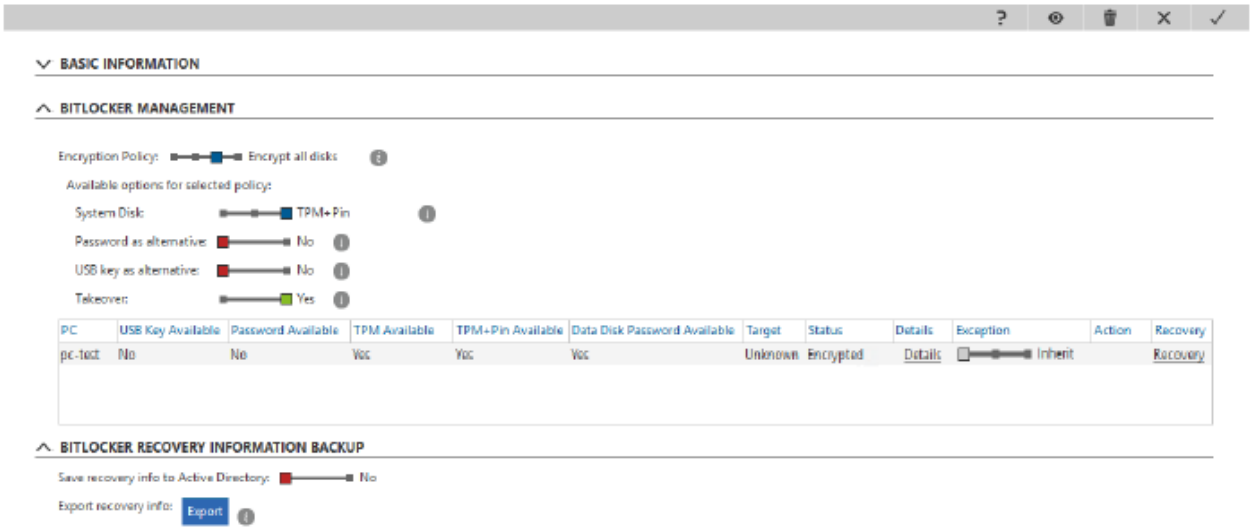
Примечание. USB-накопитель автоматически разблокируется даже на компьютере с установленной консолью.

Экспорт паролей

Пароли для флеш-накопителей можно экспортировать. Выберите в списке соответствующие флеш-накопители, которые зашифрованы, нажмите *Экспорт* и сохраните таблицу CSV с паролями.

4.6.8. Диски BitLocker

BitLocker используется для физического шифрования любых системных дисков и дисков данных, подключенных к компьютерам. Это инструмент Microsoft. Более подробная информация о BitLocker доступна по ссылке.



Примечание. Шифрование диска Bitlocker можно использовать только на конечных рабочих станциях с Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Pro и Windows 8 Enterprise, Windows 10 Pro и более новыми операционными системами Windows, включая версии серверов. Bitlocker не совместим с динамическими дисками.

Управление BitLocker

Политика шифрования

Здесь вы можете настроить политику BitLocker. Выбранная политика будет применяться и внедряться на перечисленных ниже компьютерах, если они поддерживают выбранную политику. Для тех компьютеров, которые ее не поддерживают, можно выбрать другие варианты. Доступны следующие политики:

- *Расшифровать* — расшифровывает системный диск и все диски данных.
- *Шифрование всех дисков* — шифрует системный диск с помощью выбранного метода (см. далее) и шифрует диск данных с помощью случайным образом сгенерированных ключей. Диски данных разблокируются автоматически после разблокировки системного диска.
- *Шифрование дисков* — шифрование применяется только к дискам данных.

Настройте одну из следующих опций в соответствии с выбранной политикой:

- *Системный диск* — выбор метода разблокировки системного диска:
    - *Пароль. При запуске ПК пользователю предлагается ввести пароль, установленный пользователем при применении политики.*
    - *TPM. Системный диск будет автоматически разблокирован при запуске. Пароль хранится на модуле защиты TPM.*
    - *TPM+Pin. Пароль хранится на модуле защиты TPM с дополнительной защитой PIN-кодом. При запуске ПК пользователю предлагается ввести PIN-код, установленный пользователем при применении политики.*
- *Пароль как альтернатива* — пароль будет установлен как альтернативный способ разблокировки системного диска. Этот вариант можно настроить только в том случае, если выбран метод разблокировки TPM или TPM+Pin.

Примечание. Этот вариант доступен только на компьютерах с системой Windows 8 и более поздних версий.

- *USB-ключ как альтернатива* — ключ, хранящийся на USB-накопителе, будет установлен как альтернативный способ разблокировки системного диска.

  Примечание. Этот вариант доступен только на компьютерах с ОС Windows Vista и 7+.

- *Перенимать* — Safetica принимает под свой контроль диски, ранее зашифрованные с помощью BitLocker, но без участия Safetica. Старые имя для входа и ключи восстановления будут удалены и заменены новыми в соответствии с установленной политикой. Если этот параметр не активен, некоторые попытки шифрования могут завершиться ошибкой.

Список компьютеров

Список включает все компьютеры, на которых установлена Safetica, и содержит группы, отмеченные в дереве пользователей. Для каждого компьютера указывается подробная информация о текущем состоянии BitLocker на соответствующем компьютере. Например, какие конкретные параметры безопасности BitLocker поддерживает компьютер и зашифрован ли он.

Для каждого компьютера можно установить исключение:

- *Игнорировать* — политика шифрования не будет применяться к соответствующему компьютеру.
- *Расшифровать* — все диски на соответствующем компьютере будут зашифрованы.

Вы можете установить исключение, используя переключатель в столбце с тем же именем.

Резервная копия информации о восстановлении BitLocker

В этом разделе вы можете настроить резервное копирование информации в Active Directory или экспорт в указанную папку. Резервное копирование в Active Directory нужно включить.

Примечание. Если данные, необходимые для восстановления, были экспортированы в корневую папку подключенного USB-диска, этот диск можно использовать для восстановления доступа к зашифрованному диску.

5. Клиент

5.1. Диалоги оповещений

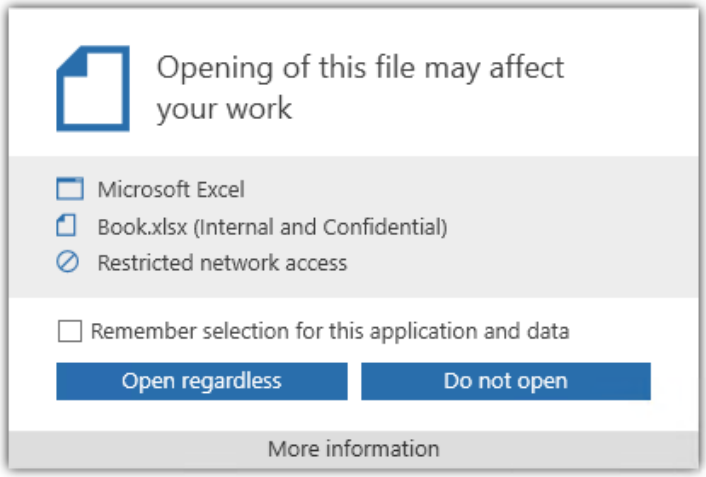
Safetica Protection и Safetica Enterprise отображают информацию для пользователей о запрещенных или разрешенных действиях с помощью диалоговых окон. Диалоги отображаются в правом нижнем углу рабочего стола. Существует множество типов таких диалогов. Каждый диалог требует различного взаимодействия с пользователем (подтверждение, отклонение, выбор из опций или путей).

Пример диалога оповещения:

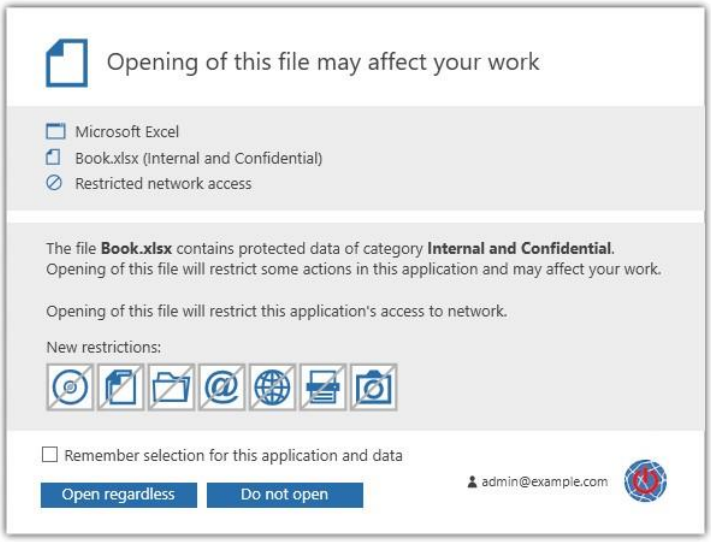
Щелкнув ссылку *Подробнее*, вы увидите более подробную информацию:

Оповещение при работе с защищенными данными

Когда пользователь открывает данные, защищенные политикой безопасности, появляется диалоговое окно с информацией:



Нажмите *More information (Дополнительная информация),* чтобы увидеть более подробную информацию об ограничениях, применяемых к приложению:



Следующие пиктограммы обозначают запреты или ограничения в приложении при работе с защищенными данными:

Нажав на пиктограммы, пользователь увидит объяснения соответствующих запретов или ограничений: