CryptoDetector

Краткое руководство пользователя

Версии компонентов: CryptoDetector Platform — 0.3.0.0; агент CryptoDetector — 0.0.5.6

Правообладатель: ООО «Безопасные программные решения» (ИНН 5836687096)

Содержание

1. Введение....3
1.1. Назначение документа....3
1.2. Описание программного обеспечения....3
1.3. Основные возможности....3
2. Начало работы....4
2.1. Вход в административную панель....4
2.2. Первый вход и активация лицензии....6
2.3. Рабочая станция....6
3. Работа с административной панелью (серверная платформа)....6
3.1. Обзор....7
3.2. Компьютеры....7
3.3. Списки доступа....7
3.4. Заявки....8
3.5. События....8
3.6. Аудит....8
3.7. Настройки....9
4. Работа с агентом на рабочей станции....9
4.1. Разделы приложения....9
4.2. Статус....9
4.3. Списки....10
4.4. Журнал....10
4.5. Лицензия....10
4.6. Настройки....11
4.7. Уведомления....11
5. Завершение работы....11

1. Введение

1.1. Назначение документа

Настоящее краткое руководство пользователя предназначено для ознакомления пользователей с основными операциями при работе с программным обеспечением CryptoDetector (далее — ПО).

Руководство содержит описание входа в административную панель серверной платформы и работы с её разделами, а также описание работы с агентом, установленным на рабочей станции.

1.2. Описание программного обеспечения

CryptoDetector — клиент-серверное программное обеспечение, предназначенное для мониторинга состояния объектов файловой системы, анализа и выявления их изменений, производимых с целью шифрования, а также восстановления данных указанных объектов.

ПО состоит из двух частей, работающих совместно:

• **CryptoDetector Platform (далее — Платформа)** — серверная часть; развёртывается на сервере организации; включает серверное приложение, административную панель и программный интерфейс; обеспечивает централизованное управление рабочими станциями, хранение единых списков, событий и настроек;

• **CryptoDetector (далее — агент)** — клиентская часть; устанавливается на рабочие станции под управлением операционной системы Windows; обеспечивает наблюдение за объектами файловой системы и восстановление данных; взаимодействует с Платформой (получение настроек и списков, передача событий и заявок, получение корпоративной лицензии).

1.3. Основные возможности

Возможности агента (рабочая станция):

• наблюдение за объектами файловой системы и выявление изменений, производимых с целью шифрования;

• блокирование выявленных операций с уведомлением пользователя (с возможностью разрешить конкретную операцию);

• формирование резервных копий изменяемых объектов и восстановление данных;

• ведение белого и чёрного списков объектов;

• журнал событий;

• активация и контроль лицензии;

• настройка режима работы, отслеживания ассоциированных файлов, поддержки сетевых дисков и папок.

Возможности Платформы (административная панель):

• учёт рабочих станций, подтверждение новых станций, управление статусами;

• централизованные списки доступа (белый и чёрный списки), импорт и экспорт;

• обработка заявок от рабочих станций;

• просмотр событий с рабочих станций;

• журнал аудита действий администраторов;

• системные настройки, настройки рабочих станций (общие и персональные), лицензия, уведомления по электронной почте;

• журнал изменений списков доступа (версии) и аудит действий администраторов.

2. Начало работы

2.1. Вход в административную панель

1. Откройте в браузере адрес административной панели (адрес зависит от выбранного при установке профиля подключения; например, `https://<сервер>:7291/`).

2. На странице входа заполните поля «Логин» и «Пароль» и нажмите «Войти».

3. При первой установке система потребует сменить пароль — задайте новый пароль и сохраните его (в проверочном экземпляре пароль уже задан, смена не требуется).

4. Для смены пароля в дальнейшем используйте раздел «Профиль» → «Сменить пароль».

5. Для выхода из системы нажмите «Выйти».

Параметры доступа к проверочному экземпляру ПО (для экспертной проверки):

• операционная система виртуальной машины: учётная запись `VM`, пароль `0000`;

• административная панель: `https://localhost:7291/` (на виртуальной машине) или `https://<IP-адрес виртуальной машины>:7291/` (с внешнего компьютера; при подключении по IP-адресу браузер сообщит о самоподписанном сертификате — предупреждение необходимо принять);

• учётная запись административной панели: логин `admin`, пароль `adminadmin`.

Пароль распаковки архива с образом виртуальной машины и полный состав экземпляра приведены в руководстве по установке (раздел 10).

Порядок работы с проверочным экземпляром:

1. Развернуть виртуальную машину из архива, запустить её и войти в операционную систему.

2. Открыть административную панель и войти (см. параметры доступа выше).

3. Открыть приложение администратора рабочей станции (ярлык «CryptoDetector» в меню «Пуск») и на вкладке «Статус» включить переключатель «Защита от шифрования» — наблюдение начнёт работу.

4. По завершении проверки выключить переключатель «Защита от шифрования» и завершить работу операционной системы обычным способом.

2.2. Первый вход и активация лицензии

В проверочном экземпляре лицензия уже активирована — приведённые ниже шаги требуются только при самостоятельной установке ПО.

1. При первой установке вход выполняется учётной записью по умолчанию: логин **Admin**, пароль **admin** — система сразу предложит сменить пароль. В проверочном экземпляре пароль администратора уже задан (см. параметры доступа в разделе 2.1), смена пароля не требуется.

2. Откройте «Настройки» → вкладка «Лицензия» → «Выбрать файл» — укажите предоставленный файл лицензии → «Загрузить лицензию».

3. До активации лицензии функциональность системы ограничена (в панели отображается предупреждение).

2.3. Рабочая станция

На рабочей станции установлены: служба `CDService` (работает автоматически), приложение администратора рабочей станции и компонент уведомлений. Окно приложения администратора рабочей станции содержит разделы: «Статус», «Списки», «Журнал», «Лицензия», «Настройки».

При загрузке операционной системы служба запускается автоматически; если наблюдение было включено, оно также возобновляется автоматически (при наличии активной лицензии). Включение и выключение наблюдения выполняются переключателем «Защита от шифрования» на вкладке «Статус».

Агент работает совместно с Платформой: рабочая станция регистрируется на Платформе, передаёт на сервер события и заявки, получает единые списки и настройки; при корпоративном режиме лицензия агента предоставляется Платформой. Возможна и автономная работа агента — с активацией лицензии файлом и локальным ведением списков.

3. Работа с административной панелью (серверная платформа)

Меню панели содержит разделы: «Обзор», «Компьютеры», «Списки доступа», «Заявки», «События», «Аудит», «Настройки». Язык интерфейса и

тема оформления («Светлая», «Тёмная», «Системная») переключаются в верхней части панели (в шапке), рядом с меню пользователя.

3.1. Обзор

Раздел «Обзор» отображает сводную информацию: количество компьютеров, последнее обновление списков, активные заявки, последние события. Для перехода к полному списку событий используйте ссылку «Все события».

3.2. Компьютеры

Раздел «Компьютеры» содержит перечень рабочих станций, зарегистрированных на Платформе, с фильтром по статусу («Ожидает», «Активен», «Заблокирован») и поиском по компьютеру. В списке отображаются: идентификатор станции, имя компьютера, статус и число событий. Карточка станции содержит: имя компьютера, идентификатор, версию ПО, аппаратный идентификатор (Hardware ID), IP-адрес, дату создания и время последнего входа, а также вкладки «События» и «Настройки компьютера».

• **Подтверждение новой станции.** Новые станции отображаются со статусом «Ожидает»; откройте станцию и измените статус на «Активен» («Изменить статус»).

• **Блокирование станции.** Изменение статуса на «Заблокирован» ограничивает доступ станции к данным Платформы.

• **Персональные настройки.** «Настройки компьютера» — задайте значения, отличные от общих; «Сбросить к глобальным» возвращает наследование общих настроек.

• **Удаление.** «Удалить компьютер» — станция удаляется из списка.

3.3. Списки доступа

Раздел «Списки доступа» предназначен для ведения единых белого и чёрного списков объектов (по значению хеша). Раздел содержит вкладки «Записи» и «Журнал изменений».

• **Добавление записи.** Нажмите «Добавить запись», укажите список (белый/чёрный), хеш и описание.

• **Изменение описания.** Кнопка «Редактировать» в строке записи.

• **Удаление.** Кнопка «Удалить» в строке записи (с подтверждением).

• **Импорт.** Кнопка «Импорт» — загрузка файла CSV (проверка выполняется предварительно: отображаются строки, коллизии и ошибки; доступны параметры обработки коллизий).

• **Экспорт.** Кнопка «Экспорт» — выгрузка выбранного списка в файл CSV.

• **Журнал изменений.** Вкладка «Журнал изменений» отображает версии списков и операции (создание, обновление, удаление, восстановление).

3.4. Заявки

Раздел «Заявки» отображает заявки от рабочих станций на добавление объектов в списки.

1. Откройте заявку для просмотра деталей.

2. Нажмите «Одобрить заявку» — указанный хеш будет добавлен в список доступа, либо «Отклонить заявку» — обязательно укажите комментарий к отклонению.

3. Обработанные заявки отображаются со статусами «Одобрено»/«Отклонено», указывается дата обработки и кто рассмотрел.

3.5. События

Раздел «События» отображает события, поступающие с рабочих станций: «Блокировка запуска» (заблокирован запуск процесса) и «Блокировка шифрования» (заблокирована операция записи/шифрования). Для каждого события отображаются дата и время, компьютер, тип и данные события. Доступны фильтры (по компьютеру и др.) и просмотр подробной информации («Просмотр»). Отправка событий на Платформу управляется настройкой «Отправка событий активности» (раздел «Настройки»).

3.6. Аудит

Раздел «Аудит» содержит журнал действий администраторов: вход и выход, смена пароля, изменение статуса компьютеров, операции со

списками доступа, обработка заявок, изменение настроек, работа с лицензией. Доступны поиск и просмотр деталей.

3.7. Настройки

Раздел «Настройки» содержит вкладки:

• **«Системные настройки»** — «Авто-одобрение заявок», «Авто-добавление компьютеров», «Хранение событий активности», «Хранение логов». После изменения нажмите «Сохранить».

• **«Настройки компьютеров»** — общие (глобальные) настройки агентов: «Отправка событий активности», «Авто-чёрный список», «Режим защиты» («Мягкий»/«Нормальный»/«Жёсткий»), «Отслеживание ассоциированных файлов» («Все»/«Скачанные»), «Поддержка сетевых дисков и папок». После изменения нажмите «Сохранить».

• **«Лицензия»** — сведения о лицензии (статус, тип, срок действия, лимит компьютеров); кнопки «Выбрать файл»/«Загрузить лицензию» (для загрузки новой лицензии), «Заменить лицензию», «Удалить лицензию».

• **«Уведомления»** — настройка почтового сервера (адрес хоста, порт, протокол, отправитель, режим шифрования) и получателей; кнопка «Проверить соединение»; выбор типов событий для отправки.

4. Работа с агентом на рабочей станции

4.1. Разделы приложения

Приложение администратора рабочей станции содержит разделы «Статус», «Списки», «Журнал», «Лицензия», «Настройки». Рядом с заголовком отображается версия ПО. При отсутствии активной лицензии отображается сообщение «Лицензия неактивна» и кнопка «Активировать».

4.2. Статус

Раздел «Статус» содержит переключатель «Защита от шифрования» («Включение или выключение защиты»).

• Включение и выключение выполняется при активной лицензии и наличии прав администратора.

• Включённое состояние означает, что наблюдение за объектами файловой системы активно; выключенное — наблюдение приостановлено.

• Выбранное состояние сохраняется и восстанавливается при повторном запуске службы.

4.3. Списки

Раздел «Списки» содержит вкладки «Белый список» и «Чёрный список»; в таблице отображаются колонки «Файл» и «Хеш».

1. Для добавления нажмите «Добавить» и выберите файл (хеш рассчитывается автоматически) либо введите значение хеша вручную (длина хеша — 64 символа, шестнадцатеричный формат).

2. Для удаления отметьте записи и нажмите «Удалить» (с подтверждением).

3. Файл, добавленный в белый список, не может одновременно находиться в чёрном списке; при необходимости система предложит перенести запись.

4.4. Журнал

Раздел «Журнал» отображает события рабочей станции (колонки «Время», «Тип события», «Подробно»): включение и выключение защиты, блокирование запуска процессов, блокирование операций шифрования, разрешение операций пользователем, изменение конфигурации, события лицензии, действия со списками (добавление, удаление), очистка журнала. Кнопка «Очистить» удаляет все записи (с подтверждением); операция очистки также фиксируется в журнале.

4.5. Лицензия

Раздел «Лицензия» отображает сведения: имя компьютера, идентификатор компьютера, ключ лицензии, тип («Пробная», «Домашняя», «Коммерческая»), статус («Действует» и др.), даты начала и окончания, остаток дней.

• Для активации нажмите «Активировать» и выберите файл лицензии (тип активации — онлайн или оффлайн).

• При корпоративном использовании лицензия предоставляется Платформой (раздел «Настройки» → «Использовать сервер внешний сервер»).

4.6. Настройки

Раздел «Настройки» содержит:

• «Язык интерфейса» — «Русский»/«English»;

• «Автоматический чёрный список» — автоматическое добавление подозрительных объектов в чёрный список;

• «Режим работы» — «Мягкий»/«Стандартный»/«Жёсткий»;

• «Отслеживание ассоциированных файлов» — «Все»/«Скачанные»;

• «Поддержка сетевых дисков и папок» — отключение CSC-драйвера (для применения требуется перезагрузка);

• «Использовать сервер внешний сервер» и «Адрес сервера» — подключение к серверной платформе (адрес в формате `ip:port` или `url`).

4.7. Уведомления

При выявлении операции, классифицированной как изменение с целью шифрования, отображается всплывающее уведомление о блокировании. Пользователь может разрешить конкретную операцию; сведения о блокировании и разрешении фиксируются в журнале.

5. Завершение работы

• **Административная панель.** Для завершения сеанса нажмите «Выйти». Серверные службы продолжают работу.

• **Рабочая станция.** Закрытие окна приложения администратора не останавливает службу: наблюдение продолжается. Полная остановка работы ПО на рабочей станции выполняется администратором через оснастку «Службы» (остановка службы `CDService`).