Safe'n'Sec

Продуктовая линейка 3.11

Примечания к выпуску

Введение

Назначение

Продуктовая линейка 3.11 компании Safe'n'Sec предлагает набор программных компонентов для развёртывания системы информационной безопасности. Система предназначена для обеспечения целостности программной среды конечных точек сети и защиты данных от несанкционированного доступа со стороны обслуживающего персонала или злоумышленников.

В продуктовую линейку входят следующие модули:

- Safe'n'Sec Service Center («Сервисный Центр») в составе:
  - Safe'n'Sec Server - серверный компонент;
  - Safe'n'Sec Admin Console - консоль управления;
- Safe'n'Sec ATM Client / Endpoint Client / SClient / SysWatch Personal (далее по тексту - «Safe'n'Sec SysWatch») - клиентские компоненты проактивной защиты устройств самообслуживания, рабочих станций корпоративной сети, серверов и персональных компьютеров соответственно;
- Safe'n'Sec DLP Client - клиентский компонент мониторинга и сбора данных об активности пользователя.

Настоящий документ представляет основные изменения и новые возможности, вошедшие в версию 3.11.

Версия 3.11

Улучшения и новые возможности:

Устранённые дефекты:

Улучшения и новые возможности

Удалённая настройка белого списка сертификатов

В Сервисном Центре 3.11 стало возможным удалённо управлять белым списком сертификатов, используемым клиентским модулем Safe'n'Sec SysWatch для контроля запуска программ установки по их ЭЦП.

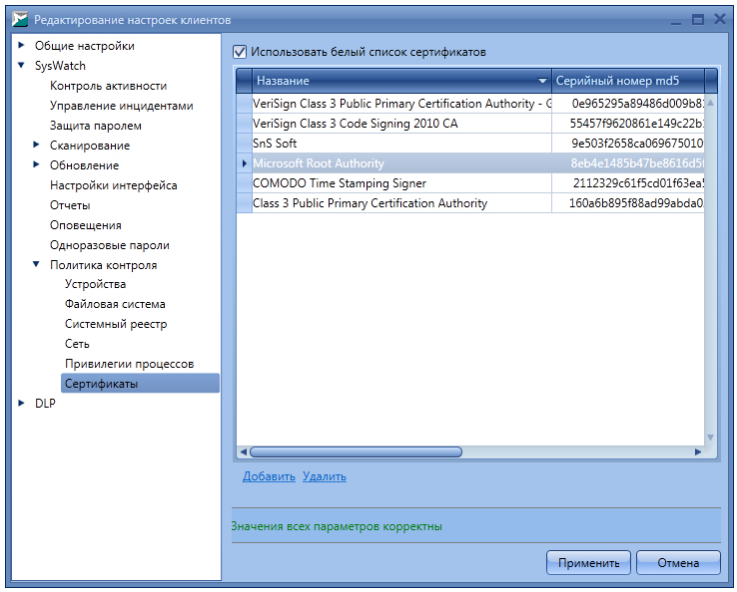

Рисунок 1. Белый список сертификатов

Настройка списка осуществляется в клиентской конфигурации и происходит аналогично локальной работе в интерфейсе Safe'n'Sec SysWatch (рис. 1). Таким образом стало возможным удалённо вырабатывать и применять единую политику по контролю сертификатов для каждого клиентского подразделения (всех подразделений).

Логирование блокировки DLL-модулей

В версии 3.11 реализовано логирование существующего функционала Safe'n'Sec SysWatch по контролю DLL-модулей, загружаемых исполняемыми компонентами. Запись о событии блокировки модулей теперь ведётся как в локальные текстовые отчёты Safe'n'Sec SysWatch, так доступно и администратору отдельным событием в консоли управления Safe'n'Sec Admin Console (рис. 2).

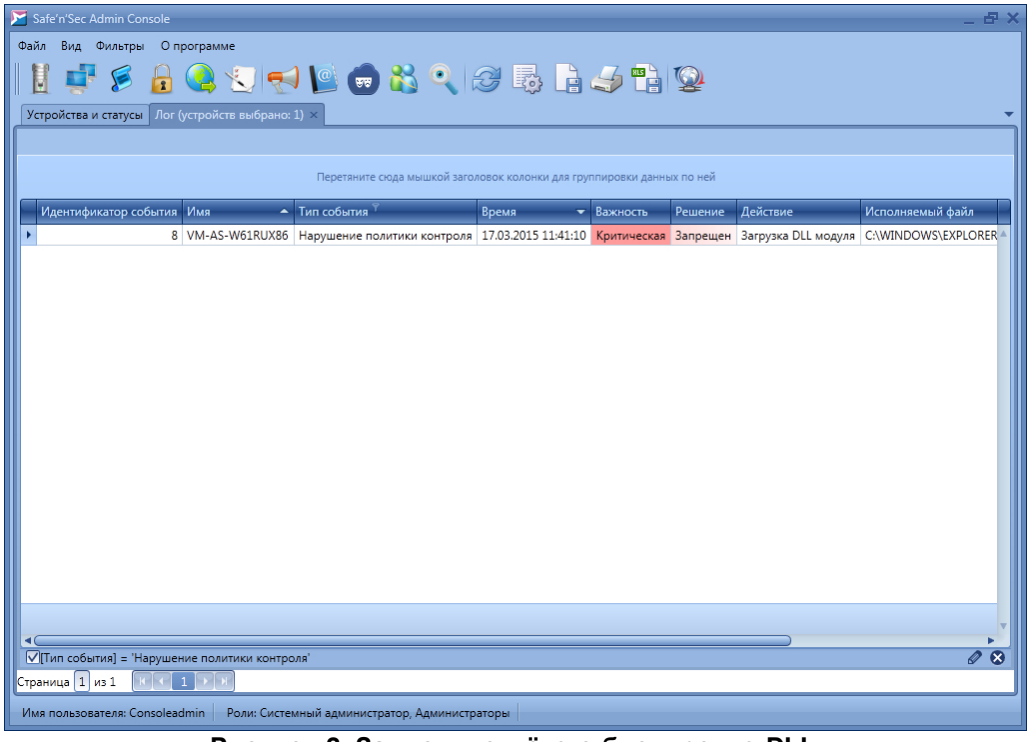

Рисунок 2. Запись в отчёте о блокировке DLL

Запись видео при возникновении инцидентов

Клиентский модуль сбора данных Safe'n'Sec DLP Client версии 3.11 позволяет захватывать снимки экрана компьютера в момент возникновения инцидентов (совершения действий над наблюдаемыми объектами). Снимки передаются на сервер Сервисного Центра и централизованно хранятся в его базе данных. Последовательность снимков

может быть воспроизведена в качестве видеозаписи администратором через консоль управления Safe'n'Sec Admin Console. Видеозапись вызывается через контекстное меню соответствующего события в отчётах Safe'n'Sec DLP Client (рис. 3, 4).

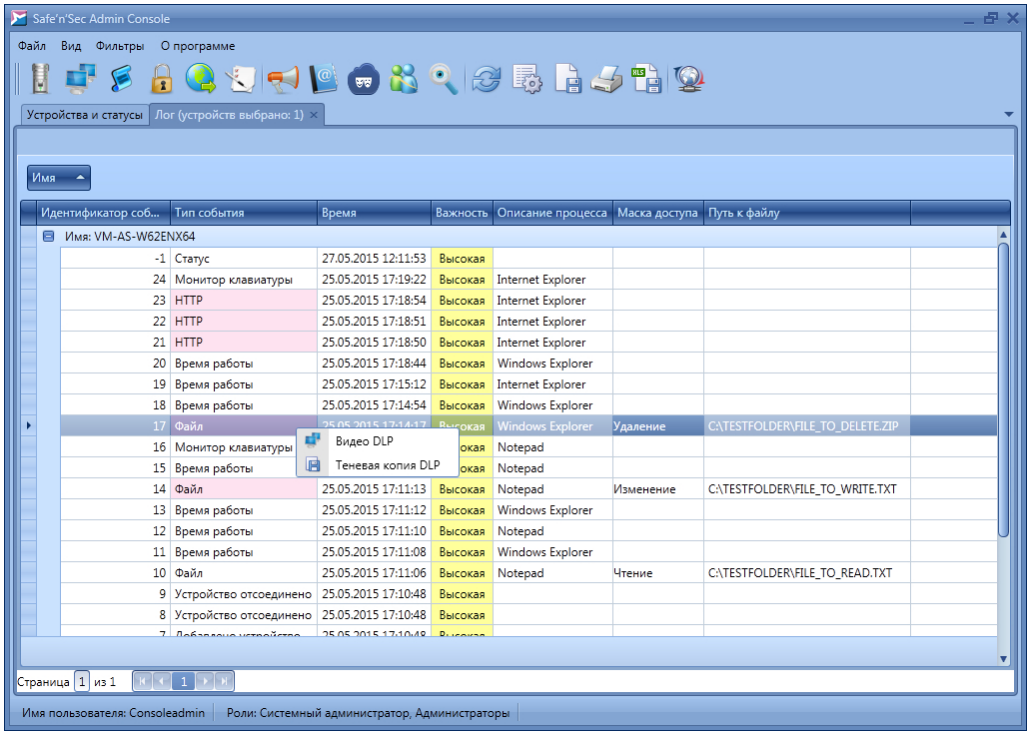

Рисунок 3. Вкладка "Лог" для компонента Safe'n'Sec DLP Client

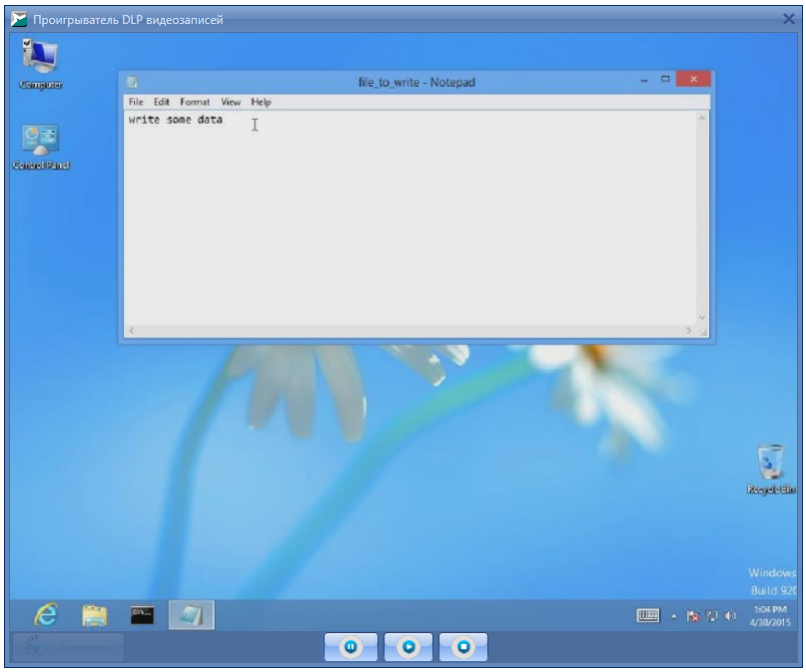

Рисунок 4. Проигрыватель видеозаписей Safe'n'Sec DLP Client

Администратору доступны настройки параметров сохранения снимков в

конфигурации клиентского модуля (рис. 5).

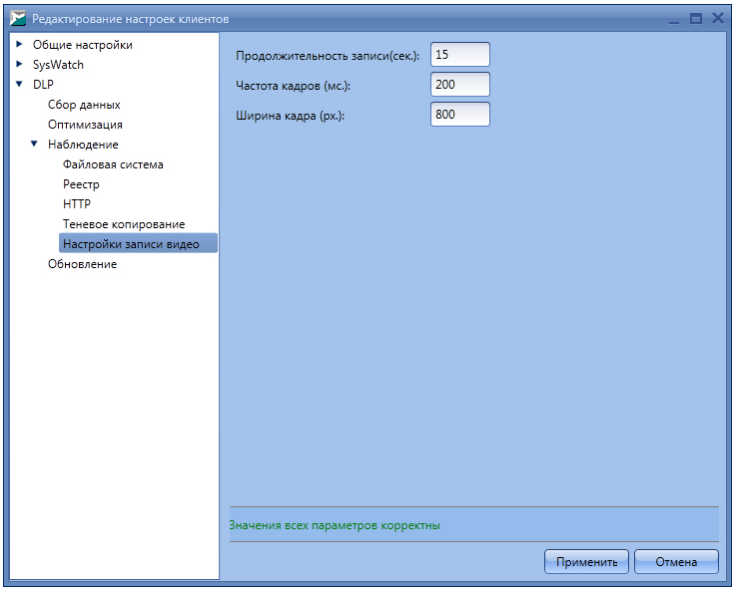

Рисунок 5. Настройки записи видео

Следующие наблюдаемые события могут быть отслежены с помощью захвата снимков экрана:

- чтение объектов файловой системы / системного реестра;
- создание объектов файловой системы / системного реестра;
- изменение объектов файловой системы / системного реестра;
- переименование объектов файловой системы / системного реестра;
- удаление объектов файловой системы / системного реестра;
- передача данных по сети.

Удалённый доступ к теневым копиям

В Сервисном Центре 3.11 стало возможным удалённо получить доступ к теневым копиям наблюдаемых объектов, сохраняемых клиентскими модулями Safe'n'Sec DLP Client. Администратору доступна резервная копия изменённого объекта наблюдения в консоли управления Safe'n'Sec Admin Console через контекстное меню соответствующего события в отчётах Safe'n'Sec DLP Client (рис. 3, 6).

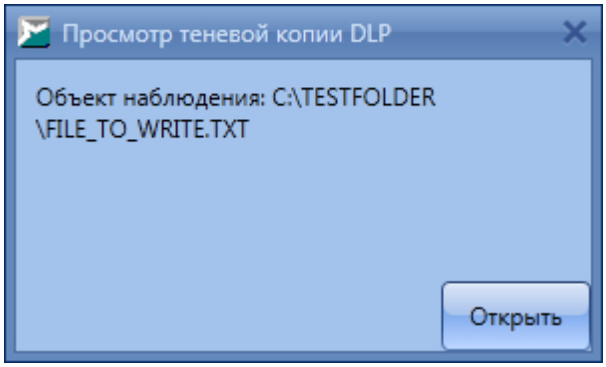

Рисунок 6. Теневая копия объекта наблюдения

Централизованное обновление клиентских модулей по требованию

В Сервисном Центре версии 3.11 доступна новая возможность, расширяющая возможности централизованного обновления клиентских модулей системы информационной безопасности. Теперь помимо удалённого обновления посредством задания расписания, администратору Safe'n'Sec Admin Console доступно удалённое обновление по требованию с помощью нового соответствующего вида задач. В качестве опций задачи можно выбрать обновляемые компоненты, а также выбрать выполнять ли принудительную перезагрузку клиентских устройств после обновления (рис. 7).

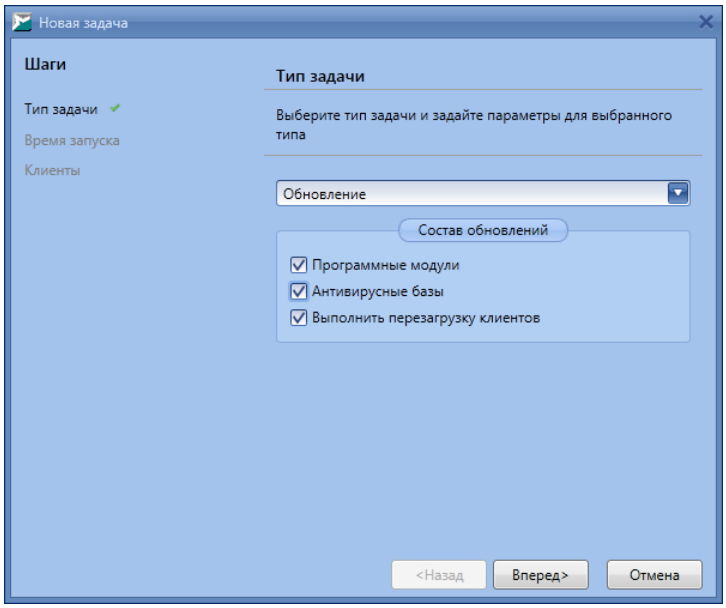

Рисунок 7. Опции задачи обновления

Новые инсталляторы Safe'n'Sec SysWatch и Safe'n'Sec DLP Client

В клиентских модулях Safe'n'Sec SysWatch и Safe'n'Sec DLP Client версии 3.11

применены новые инсталляторы, что для конечных пользователей обеспечило возможность мультиязыковой установки компонентов и упрощённую процедуру обновления. Помимо этого, облегчен сам процесс разработки инсталляторов и их сопровождения. Исполнение инсталляторов серверных и клиентских компонентов в одной технологии позволяет организовать однородную и логичную структуру на сервере обновлений Safe'n'Sec.

Устранённые дефекты

Safe'n'Sec SysWatch: неполное слияние политик от СЦ и локальных политик

При применении правил, полученных от Сервисного Центра, на клиенте Safe'n'Sec SysWatch не происходило удаление части локальных политик (частных правил).

Решение:

Устранено в версии 3.11. Слияние политик от Сервисного Центра и текущих локальных политик происходит корректно.

Safe'n'Sec SysWatch: ошибка подсчёта хеш-суммы приложения, имеющего некорректный формат PE

Было установлено, что драйвер Safe'n'Sec SysWatch не высчитывает хеш-сумму исполняемого файла, имеющего некорректный формат PE. В результате запуск подобных приложений блокировался во всех случаях.

Решение:

Особенность устранена в версии 3.11. Исполняемые файлы с некорректным форматом PE обрабатываются драйвером в штатном порядке.

Safe'n'Sec Service Center: ошибка при удалении клиента из базы данных

При удалении клиентских модулей Safe'n'Sec SysWatch из базы данных Сервисного Центра возникала ошибка в консоли управления Safe'n'Sec Admin Console в случаях большого количества накопленных событий в отчётах (250 000 записей и более).

Решение:

Алгоритм удаления клиентских модулей из базы данных был оптимизирован в версии

3.11 для исключения подобных ошибок.

Safe'n'Sec Service Center: аварийное завершение работы консоли управления при удалении всех политик файловой системы

В случае удаления всех правил из политики контроля файловой системы в конфигурации Safe'n'Sec SysWatch происходило аварийное завершение работы консоли управления Safe'n'Sec Admin Console.

Решение:

Устранено в версии 3.11.

Техническая поддержка

При возникновении вопросов по установке, настройке и работе продуктов Safe'n'Sec Вы можете обращаться в техническую поддержку по электронной почте support@safensoft.ru в круглосуточном режиме.