ГАЗИНФОРМ СЕРВИС

Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v. 4

Описание релиза v. 4.14.100

Санкт-Петербург, 2023

Описание релиза программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4.14.100

Программный комплекс «Efros Config Inspector» релиз 4.14.100 (далее – ПК «Efros Config Inspector» v.4).

О релизе:

Основные нововведения релиза:

- добавлена поддержка Eltex WLC;
- добавлена поддержка Weidmueller;
- добавлена поддержка SCADA Alpha.HMI;
- добавлена поддержка ПЛК Trei (QNX 6.5);
- добавлена поддержка ПЛК Ezan (QNX 6.5);
- добавлена поддержка Time-range для Eltex MES;
- добавлены HitCount для устройств Dionis NX;
- добавлена операция экспорта настроек по расписанию;
- добавлена поддержка работы с sub интерфейсами для Check Point;
- добавлена поддержка работы с sub интерфейсами для Eltex MES;
- добавлена ссылка для получения информации о системе для техподдержки;
- добавлена ссылка для получения логов сервера для техподдержки;
- добавлена поддержка режима policy based для Fortinet FortiGate.

Также добавлен ряд функциональных улучшений. Выполнены доработки для упрощения работы пользователей и оптимизации системы.

Новые возможности

1 Добавлена поддержка Eltex WLC

В разделе **Настройки – *Модули*** в модуль *Eltex* добавлен новый тип устройства *Eltex WLC*.

2 Добавлена поддержка Weidmueller

В разделе **Настройки – *Модули*** добавлен новый модуль *Weidmueller* с типом устройства *Weidmueller AdvancedLine*.

3 Добавлена поддержка SCADA Alpha.HMI

В разделе **Настройки – *Модули*** добавлен новый модуль *Alpha.HMI* с типом устройства *SCADA Alpha.HMI* (производитель ***Атомик Софт***).

4 Добавлена поддержка ПЛК Trei (QNX 6.5)

В разделе **Настройки – *Модули*** добавлен новый модуль *ПЛК Trei* с типом устройства *ПЛК Trei (QNX 6.5)* (производитель ***АО «ТРЭИ»***).

5 Добавлена поддержка ПЛК Ezan (QNX 6.5)

В разделе **Настройки – *Модули*** добавлен новый модуль *ПЛК Ezan* с типом устройства *ПЛК Ezan (QNX 6.5)* (производитель ***АО «ЭЗАН»***).

6 Добавлена поддержка Time-range для Eltex MES

Для устройств типа *Eltex MES* в отчеты по правилам МЭ в колонку ***Additional*** добавлены *Time range*.

7 Добавлены HitCount для устройств Dionis NX

Добавлена проверка активности правил HitCount для устройств *Dionis NX*.

8 Добавлена операция экспорта настроек по расписанию

В разделе **Настройки – *Расписания*** добавлен новый тип расписания (тип операции в окне добавления расписания) *Экспорт настроек.*

Для расписания задаются:

1. Стандартные настройки расписаний – активность, имя, описание и временные параметры.
2. Способ экспорта – два варианта:
   - *Локальная папка* – экспорт в локальную папку на сервере ПК «Efros Config Inspector» v.4 с указанием пути (в формате для win и для lin);
   - *Удаленно по SFTP* – экспорт в директорию на удаленном сервере SFTP с указанием пути до директории (в формате для win и для lin), адреса и порта удаленного сервера, а также пользователя и пароля.

Для удаленного подключения есть возможность проверки подключения.

3. Экспортируемые настройки (параметры профилей, проверок и отчетов, параметры стандартов проверок МЭ и список устройств) и защита файла настроек – полностью аналогично настройкам экспорта в разделе **Настройки** – ***Экспорт настроек.***

По умолчанию выполняется экспорт всех настроек.

9 Добавлена поддержка работы с sub-интерфейсами для Check Point и Eltex MES

В унифицированный отчет ***Интерфейсы*** добавлен вывод sub интерфейсов из основной конфигурации.

10 Ссылки для получения информации о системе и для получения логов сервера для техподдержки

В окне просмотра сведений о ПК «Efros Config Inspector» v.4 (открывается после нажатия в заголовке клиентской консоли кнопки  и выбора в открывшемся меню пункта ***О программе***) добавлены ссылки:

– *Логи сервера* – для скачивания логов сервера ПК в виде архива (ссылка доступна для пользователей комплекса с правами *Просмотр* или *Управление* категории *Администрирование*);

– *Сведения о системе* – для просмотра характеристик комплекса, с возможностью копирования текста для дальнейшей передачи в техподдержку (ссылка доступна только для пользователей комплекса с правами *Управление* категории *Администрирование*).

11 Поддержка режима policy based для Fortinet FortiGate

Для устройств Fortinet FortiGate добавлена поддержка работы с policy based mode без и с VDOM.

12 Доработки интерфейса

Выполнены доработки интерфейса консоли для упрощения работы пользователей:

– во вкладке ***Отчеты*** для устройств в разделе **Устройства** добавлена индикация неактуальности отчета для отчетов проверок МЭ (отчет оптимизации правил, отчеты зонного анализа и отчет стандартов МЭ) – пиктограмма «  » и всплывающая подсказка *Настройки проверки изменились, для получения актуальных данных обновите отчет*. В форме просмотра такого отчета отображается баннер с тем же сообщением и кнопкой **Обновить** для обновления отчета. После обновления отчета пиктограмма исчезает. Если требующий обновления отчет открыт одним пользователем, а другой одновременно с этим запустил операцию обновления отчета, то текст сообщения изменится на *Доступна свежая версия текущего отчета*;

– для устройств Primo RPA (Robot, Stuio, Orchestrator) доработаны названия и логика:

а) для всех типов устройств за исключением host в указании пути (путь по умолчанию) название изменено на "Путь Primo RPA *", где * – Robot, Stuio или Orchestrator в зависимости от типа
б) для Primo RPA Robot изменено название строки с указанием пути до конфигурационного файла на "Имя конфигурационного файла". Полный путь до файла формируется путем объединения двух полей (папка и сам файл).

13 Общие доработки

Выполнены следующие доработки для оптимизации системы:

– в разделе **Отчеты** в окне просмотра отчета ***Правила межсетевых экранов*** выполнена доработка счетчика для отчетов с правилами, отключен общий лимит. Сделан лимит в 1000 записей для устройств, при достижении лимита для устройства отображаются только первые 1000 правил и сообщение *Достигнут лимит вывода данных, отображены только первые 1000 правил*;

– отключена остановка сервера ПК при возникновении критичных ошибок:
  а) из вкладки ***Дополнительно*** окна настройки сервера под MS Windows и Linux удален чекбокс *Продолжать работу сервера в случае нарушения внутренней целостности данных*;
  б) в разделе **Настройки** – ***Обработчики событий*** добавлен встроенный триггер на критичные ошибки сервера;

– добавлена поддержка формирования архива с логами функционирования сервера и выдача его по REST запросу;

– в разделе **Настройки** – ***Модули*** добавлено окно с предупреждением об удалении проверок безопасности, связанных с шаблонами обновляемого модуля, и списком проверок безопасности (требований), которые необходимо удалить. Пользователь имеет возможность подтвердить удаление проверок и продолжить обновление модуля или отменить обновление модуля;

– для устройств Vipnet Coordinator HW5 выполнена доработка контроля правил МЭ;

– для устройств Check Point внести правки в выполнение проверок безопасности, убраны нерабочие правила и выключен отчет по умолчанию в профиле;

– для устройств Check Point Check Point добавлена поддержка работы с sub интерфейсами;

– в разделе **Настройки** – ***Проверки безопасности*** в экспорт требований добавлена информация из поля *Как исправить.*