КОД безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.9

Инструкция

Управление "Континент. Универсальный коннектор"

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

АПКШ	Аппаратно-программный комплекс шифрования
КШ	Криптографический шлюз
ОС	Операционная система
ПУ	Программа управления
РМ	Рабочее место
СУ	Сетевое устройство
ЦУС	Центр управления сетью

Введение

Программный модуль "Континент. Универсальный коннектор" (далее — коннектор) предназначен для выгрузки конфигурации сетевых устройств АПКШ "Континент" (далее — комплекс), формирования XML-файлов для анализа системой Skybox Security (далее — Skybox) и Efros Config Inspector (далее — Efros).

Внимание! Коннектор совместим только со Skybox Security версий 10 и 11.

Выгрузка конфигураций осуществляется в соответствии с заданным расписанием или по команде администратора.

Развертывание коннектора

Возможны следующие варианты размещения коннектора в составе комплекса:

- коннектор и ПУ ЦУС функционируют на одном компьютере (РМ администратора);
- коннектор функционирует на отдельном компьютере.

Компьютер, на который устанавливается коннектор, должен соответствовать требованиям, приведенным в таблице ниже:

Элемент	Параметры
Операционная система	Windows Server 2012 R2 x64; Windows Server 2016 x64; Windows 7 SP1 x86/x64 (кроме всех выпусков Starter и Home Edition); Windows 8.1 x86/x64 (кроме всех выпусков Starter и Home Edition); Windows 10 x86/x64 (кроме всех выпусков Starter и Home Edition)
Процессор	В соответствии с требованиями ОС, установленной на компьютер
Оперативная память	Не менее 2 Гбайт
Жесткий диск (свободное пространство)	Не менее 2 Гбайт
Порты (свободные)	1 x USB 2.0 – при использовании USB-флеш-накопителя
Сетевой адаптер	Ethernet

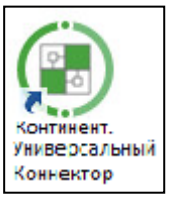
Развертывание коннектора состоит из следующих этапов:

- Установка коннектора "Континент. Универсальный коннектор".
- Создание в ПУ ЦУС администратора с ролью "Аудитор".
- Создание в Менеджере ключей ключа для подключения к ЦУС.

Для установки коннектора "Континент. Универсальный коннектор":

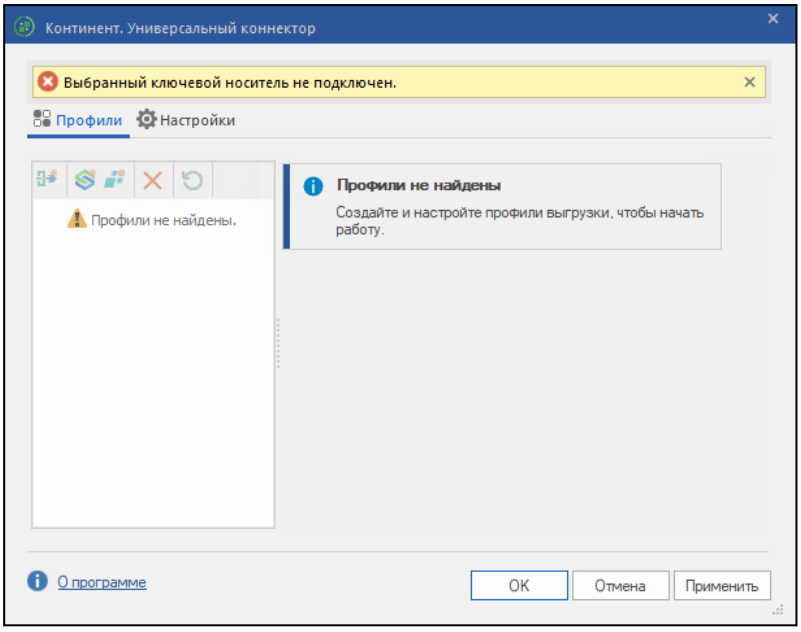
1. Запустите файл setup.exe из состава дистрибутива.
2. Установите коннектор, следуя указаниям в мастере установки.

   По окончании установки в списке "Программы" главного меню Windows и на рабочем столе компьютера появится ярлык коннектора:



3. Запустите коннектор от имени администратора.

   На экране отобразится главное окно программы.



Для создания пользователя:

1. Запустите ПУ ЦУС.
2. В списке объектов ЦУС выберите раздел "Администраторы".
3. Нажмите кнопку "Создать администратора".
4. Установите значения для следующих параметров:
   - Название — укажите название учетной записи администратора;
   - Роль — в раскрывающемся списке выберите значение "Аудитор";
   - Ключ администратора действителен до — в календаре установите срок действия ключа администратора.

   Примечание. Учетные записи администраторов с другими ролями не могут использоваться для работы коннектора.
5. Нажмите кнопку "ОК".

   На экране появится окно ввода пароля.
6. Введите пароль для шифрования ключей и нажмите кнопку "ОК".

   На экране отобразится окно записи ключевого носителя.
7. Предъявите чистый носитель для записи ключа администратора.
8. В окне выбора носителя выберите носитель для записи ключа администратора и нажмите кнопку "ОК".

   Окно создания пользователя закроется.

Для создания ключа:

1. Запустите "Менеджер ключей".
2. В раскрывающемся списке выберите носитель, на котором был записан ключ администратора с ролью "Аудитор".
3. В списке ключей выберите ключ администратора с ролью "Аудитор".
4. Нажмите кнопку "Создать ключ".
5. В окне создания ключа установите значения следующих параметров:
   - IP-адрес ЦУС;
   - Старый пароль — пароль, заданный при создании ключа;
   - Новый пароль — введите и подтвердите пароль, который будет использоваться в коннекторе для подключения к ЦУС.
6. Нажмите кнопку "ОК".

   Окно создания ключа закроется.

Начало работы

Настройка коннектора

Перед началом работы с коннектором необходимо выполнить следующие действия:

- Подключить ключевой носитель с ключом администратора с ролью "Аудитор".
- Создать профиль ЦУС.
- Создать и настроить профили выгрузки Skybox и Efros.
- Настроить работу службы Telnet.

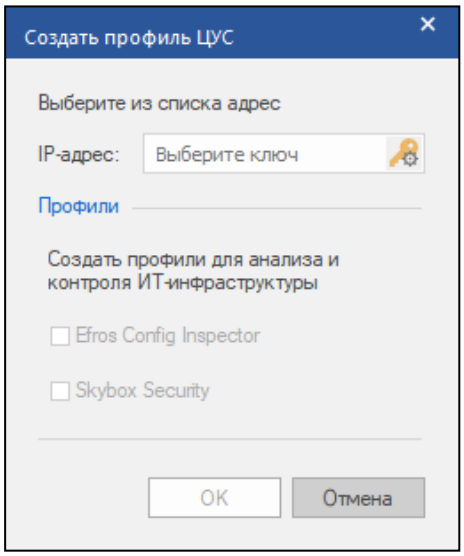
Для подключения ключевого носителя:

1. Выберите вкладку "Настройки | Приложение | Основные".
2. В раскрывающемся списке "Ключевой носитель" выберите носитель, на котором сохранен ключ администратора с ролью "Аудитор".
3. Нажмите кнопку "Применить".
4. На экране отобразится сообщение о завершении сохранения.
5. Нажмите кнопку "ОК".

Для создания профиля ЦУС:

1. Выберите вкладку "Профили".
2. Нажмите кнопку "Добавить ЦУС".

   Откроется окно создания профиля ЦУС.



3. Нажмите кнопку  .
4. Выберите в списке ключ и нажмите кнопку "ОК".

   На экране появится окно ввода пароля от ключа.
5. Введите пароль для расшифровки ключа.
6. При необходимости установите отметки в полях Efros Config Inspector и (или) Skybox Security, чтобы создать профили выгрузки конфигураций.

   Профили будут созданы вместе с профилем ЦУС и будут доступны для редактирования в разделе "Профили".
7. Нажмите кнопку "ОК".

После создания профиля ЦУС будет выполнено подключение к ЦУС.

Для создания и настройки профиля выгрузки Skybox:

1. На вкладке "Профили" нажмите кнопку .

   Примечание. Кнопка активна, только если для выбранного ЦУС не был ранее создан профиль Skybox.

2. Выберите новый профиль в списке профиля ЦУС.
3. Выберите вкладку "Основные".
4. В раскрывающемся списке выберите версию вендора.
5. В поле "Размещение" укажите путь сохранения файлов конфигурации.
6. При необходимости установите отметку в поле "Добавлять к имени файла время экспорта".
7. Выберите вкладку "КШ".
8. Нажмите кнопку .

   На экране отобразится окно со списком доступных КШ и количеством свободных лицензий.
9. В списке выберите КШ:
   - Установите отметку в строке КШ, чтобы выбрать его.
   - Нажмите кнопку , чтобы выбрать КШ по числу свободных лицензий. Будут выбраны первые КШ в списке.
   - Нажмите кнопку , чтобы снять отметки со всех выбранных КШ.
   - Нажмите кнопку , чтобы обновить список КШ.

   Выбранные КШ отобразятся в списке КШ, количество свободных лицензий обновится.
   - Чтобы удалить КШ из списка, выберите его и нажмите кнопку .
10. При необходимости установите расписание экспорта конфигураций (см. стр. **13**).

Для создания и настройки профиля выгрузки Efros:

1. На вкладке "Профили" нажмите кнопку .

   Примечание. Кнопка активна, только если для выбранного ЦУС не был ранее создан профиль Efros.

2. Выберите новый профиль в списке профиля ЦУС.
3. Выберите вкладку "Основные".
4. В поле "Размещение" укажите путь сохранения файлов конфигурации.
5. При необходимости установите отметку в поле "Добавлять к имени файла время экспорта".
6. Выберите вкладку "Устройства".
7. Нажмите кнопку .

   На экране отобразится окно со списком доступных сетевых устройств и количеством свободных лицензий.
8. В списке выберите сетевые устройства:
   - Установите отметку в строке сетевого устройства, чтобы выбрать его.
   - Нажмите кнопку , чтобы выбрать сетевые устройства по числу доступных лицензий. Будут выбраны первые сетевые устройства в списке.
   - Нажмите кнопку , чтобы снять отметки со всех выбранных сетевых устройств.
   - Нажмите кнопку , чтобы обновить список устройств.

   Выбранные устройства отобразятся в списке устройств, количество свободных лицензий обновится.

- Чтобы удалить сетевое устройство из списка, выберите устройство и нажмите кнопку ✕.

9. При необходимости установите расписание экспорта конфигураций (см. стр. **13**).

Работа с шаблонами

В коннекторе предусмотрена возможность настройки шаблонов. В шаблоне можно установить значения для следующих параметров:

- версия вендора (для Skybox);
- пути сохранения файлов конфигурации;
- добавление времени экспорта конфигурации к имени файла конфигурации;
- параметры расписания (аналогичны параметрам расписания в профилях Skybox и Efros).

Значения параметров из шаблонов будут автоматически установлены для всех создаваемых профилей ЦУС.

Для настройки параметров экспорта:

1. В главном окне коннектора выберите вкладку "Настройки".
2. В списке объектов выберите пункт "Базовый профиль".
3. Выберите вкладку "Основные".
4. В группе параметров "Вендор" выберите в раскрывающемся списке версию вендора.
5. Задайте пути сохранения файлов конфигураций для Skybox и Efros.
6. При необходимости установите отметки в полях "Добавлять к имени файла время экспорта".
7. Нажмите кнопку "Применить", чтобы сохранить настройки.

Для настройки параметров расписания:

1. Выберите вкладку "Настройки | Базовый профиль| Расписание".
2. Выберите тип расписания и установите значения необходимых параметров. Параметры расписания для общего профиля идентичны параметрам расписания профилей Skybox и Efros, см. стр. **13**.

Управление лицензиями

Управление лицензиями осуществляется на вкладке "Профили | <Имя КШ с ЦУС>| Лицензии". Файлы лицензий для коннектора хранятся локально на компьютере, на котором установлен коннектор.

Для добавления лицензии в профиль:

1. Выберите вкладку "Профили | <Имя КШ с ЦУС>| Лицензии".
2. Нажмите кнопку .
3. Выберите файл лицензии и нажмите кнопку "ОК".

Добавленные лицензии отобразятся в списке "Лицензии КШ для формирования XML".

Для удаления лицензии:

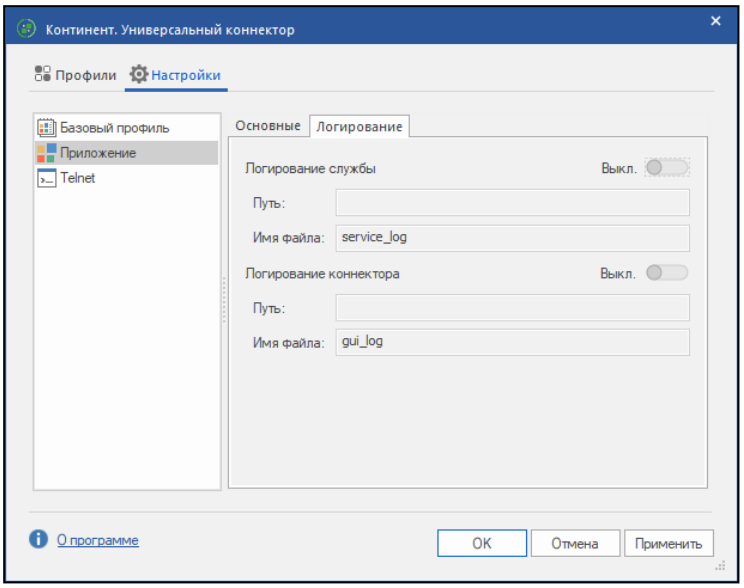
1. Выберите вкладку "Профили | <Имя КШ с ЦУС>| Лицензии".
2. Выберите файл лицензии для удаления и нажмите кнопку .

Логирование событий

В коннекторе предусмотрена возможность логирования событий службы и событий коннектора. События записываются в CSV-файлы и хранятся в указанных администратором папках.

Для включения логирования:

1. Выберите вкладку "Настройки | Приложение | Логирование".



2. Чтобы включить логирование событий службы коннектора, переведите кнопку в группе параметров "Логирование службы" в положение "Вкл".

   Параметры сохранения файла логирования станут доступными для редактирования.
3. В поле "Путь" укажите папку, в которую будет сохраняться файл.
4. При необходимости измените имя файла логирования. По умолчанию установлено имя файла "service_log".
5. Чтобы включить логирование событий коннектора, переведите кнопку в группе параметров "Логирование коннектора" в положение "Вкл".

   Параметры сохранения файла логирования станут доступными для редактирования.
6. В поле "Путь" укажите папку, в которую будет сохраняться файл.
7. При необходимости измените имя файла логирования. По умолчанию установлено имя файла "gui_log".

Экспорт конфигураций

Экспорт конфигураций может выполняться вручную или по заданному расписанию. Параметры экспорта можно настраивать для каждого профиля в отдельности или установить общие параметры для всех профилей с помощью шаблона при развертывании коннектора (см. стр. **10**).

Для экспорта конфигурации вручную:

1. На вкладке "Профили" выберите профиль Skybox или Efros.
2. Выберите вкладку "КШ" (для Skybox) или "Устройства" (для Efros).
3. В списке выберите устройство, для которого необходимо выполнить экспорт.

   Примечание. Можно выбрать несколько устройств с помощью сочетаний клавиш <Ctrl>+A, клавиш <Ctrl> и <Shift>.

4. Нажмите кнопку .

Если экспорт выполнен успешно, на экране отобразится сообщение "Экспорт успешно выполнен ". Чтобы закрыть сообщение, нажмите кнопку "ОК". Если выполнить экспорт не удалось, в журнал событий Windows будет добавлена соответствующая запись с причиной неудачи.

Для настройки периодического расписания экспорта конфигураций:

1. На вкладке "Профили" выберите профиль Skybox или Efros.
2. Выберите вкладку "Расписание".
3. Выберите вариант "Периодическое расписание".

   Параметры периодического расписания станут доступны для редактирования.
4. В поле "Каждые" укажите периодичность, с которой будет производиться экспорт.
5. В раскрывающемся списке выберите единицу времени (например, час).
6. Нажмите кнопку "Применить", чтобы сохранить настройки.

Примечание. По периодическому расписанию экспортируются конфигурации всех сетевых устройств, включенных в профиль.

Для настройки еженедельного расписания экспорта конфигураций:

1. На вкладке "Профили" выберите профиль Skybox или Efros.
2. Выберите вкладку "Расписание".
3. Выберите вариант "Еженедельное расписание".

   Параметры еженедельного расписания станут доступны для редактирования.
4. Нажмите кнопку .
5. В новой строке установите время, в которое должен производиться экспорт, и установите отметку в поле с днем недели.

   Примечание. Чтобы удалить запись из расписания, выберите запись и нажмите кнопку .
6. При необходимости повторите **пп. 4, 5**.
7. Нажмите кнопку "Применить", чтобы сохранить настройки.

Настройка службы Telnet

Для профилей Efros доступен экспорт конфигураций по запросу внешней системы по протоколу Telnet. Для корректного выполнения экспорта необходима настройка службы Telnet.

Для настройки службы Telnet:

1. В окне ОС Windows "Программы и компоненты" выберите пункт "Включение или отключение компонентов Windows".

   На экране появится окно со списком компонентов.

2. В списке компонентов установите отметки в строках служб "Клиент Telnet" и "Сервер Telnet".

   Примечание. В зависимости от версии ОС, компонент "Сервер Telnet" может отсутствовать.

3. Нажмите кнопку "ОК".
4. Запустите коннектор и выберите вкладку "Настройки | Telnet | Основные".
5. Установите значения следующих параметров для соединения с Telnet-сервером:
   - порт;
   - имя пользователя;
   - пароль.

Для запроса экспорта конфигурации:

1. Запустите коннектор и выберите вкладку "Настройки | Telnet | Основные".
2. Установите отметку в поле "Автоматический запуск", чтобы включить Telnet-сервер.
3. Подключитесь к Telnet (например, с помощью bat-файла).
4. Дождитесь запроса логина и пароля.
5. Введите логин и пароль, созданные для подключения к агенту.

   После отображения на экране фразы приветствия агент готов к работе.
6. Запросите экспорт конфигураций с помощью команды getxml.

   Синтаксис команд для экспорта см. ниже.

Конфигурации выбранных сетевых устройств будут сохранены в папки, указанные в настройках профилей.

Для запроса экспорта конфигураций доступны следующие команды:

- **profiles** — запрашивает список профилей ЦУС.

  Не требует ввода параметров. Возвращает список доступных профилей вида <ID_ЦУС> (<имя_ЦУС>).

  Пример:

```
ID455 (КШ с ЦУС)
ID456 (Kirov_CUS_01)
```

- **devicelist** — запрашивает список СУ Континент, подключенных к выбранным профилям ЦУС. Требует ввода параметра **all** либо одного или нескольких ID ЦУС, введенных через пробел:
  - **devicelist all** — запрашивает список всех СУ Континент, подключенных ко всем профилям;
  - **devicelist <ID_ЦУС> <ID_ЦУС>** — запрашивает список СУ, подключенных к выбранным ЦУС.

  Команда возвращает список СУ, привязанных к каждому выбранному профилю, с указанием имен СУ и их типов (CGW – КШ, CC – КК, IDS – ДА, NCC – ЦУС):

```
ID_ЦУС (имя_ЦУС) devices: ID_устройства|тип_устройства (имя_
устройства), ID_устройства|тип_устройства (имя_устройства)
```

  Пример:

```
ID455 (КШ с ЦУС) devices: ID477|CGW (КШ 01);
ID456 (Kirov_CUS_01) devices: ID789|CC (KK03 Rostov),
ID790|IDS (ДА);
```

- **getxml** — запрашивает XML-файлы конфигураций с выбранных СУ Континент. Требует ввода параметров:
  - **getxml all** — запрашивает XML-файлы конфигураций всех СУ, подключенных ко всем профилям ЦУС;
  - **getxml <ID_ЦУС> all** — запрашивает XML-файлы конфигураций всех СУ, имеющихся в профиле выбранного ЦУС;

- **getxml <ID_ЦУС>: <ID_СУ>,<ID_СУ>,<ID_СУ>. <ID_ЦУС>: <ID_СУ>, <ID_СУ>.** — запрашивает XML-файлы конфигураций с выбранных узлов из каждого профиля.

Сначала указывается ID ЦУС, затем через ":" и пробел указывается список СУ, привязанных к ЦУС, с которых необходимо экспортировать XML-файлы. СУ отделяются ";". Когда последнее необходимое СУ указано, ставится точка. После точки можно добавить следующий ЦУС с его СУ, отделив его от точки пробелом.

Пример:

```
getxml ID465: ID789, ID790. ID455: ID477.
```

Конфигурации сетевых устройств

Конфигурация КШ для Skybox

Конфигурации КШ сохраняются в XML-файлы, каждый XML-файл содержит конфигурацию КШ. По умолчанию название XML-файла содержит ID КШ, обозначение системы Skybox, тип КШ (CGW – КШ, NCC – КШ с ЦУС) и имя КШ. С помощью настроек профиля можно включить добавление даты и времени экспорта к имени файла.
В конфигурацию для анализа включаются сведения о следующих объектах в ЦУС:

- сетевые объекты и группы сетевых объектов;
- сервисы и группы сервисов;
- правила фильтрации, кроме правил для Усиленной фильтрации и Контроля приложений;
- правила трансляции адресов (правила NAT);
- правила статической маршрутизации.

В связи с особенностями анализа правил в Skybox Security, для КШ, функционирующего в нормальном режиме, в конец файла конфигурации добавляется запрещающее правило со следующими параметрами:

- Отправитель: любой;
- Получатель: любой;
- Действие: Отбросить.

Для КШ с включенным мягким режимом функционирования добавляется разрешающее правило со следующими параметрами:

- Отправитель: любой;
- Получатель: любой;
- Действие: Пропустить.

Имена объектов, содержащие кириллические символы, транслитерируются.

Внимание! Не присваивайте объектам в ЦУС названия, которые могут совпасть при транслитерации, например, "КШ1" и "KSH1". В таком случае в файл конфигурации будет выгружена информация только из последнего обработанного объекта с идентичным названием.

Конфигурация сетевого устройства для Efros

Конфигурации сетевых устройств сохраняются в XML-файлы, каждый XML-файл содержит конфигурацию одного устройства. По умолчанию название XML-файла содержит ID СУ, обозначение системы Efros, тип СУ (CGW – КШ, CC – КК, NCC – КШ с ЦУС, IDS – ДА.) и имя СУ. С помощью настроек профиля можно включить добавление даты и времени экспорта к имени файла.
Коннектор может экспортировать конфигурации для всех сетевых устройств комплекса версии 3.9.0 и выше. В конфигурацию для анализа включаются сведения о следующих объектах в ЦУС:

- общие параметры сетевого устройства;
- индивидуальные параметры сетевого устройства (КШ с ЦУС, КШ, КК, ДА, СД);
- сетевые объекты и группы сетевых объектов;
- сервисы и группы сервисов;
- пользователи и группы пользователей;
- временные интервалы;
- классы трафика;
- правила фильтрации;
- правила трансляции адресов (правила NAT);
- правила статической маршрутизации.