



КОД
безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.9

Инструкция

Управление коннектором "Континент-Skybox"



© Компания "Код Безопасности", 2021. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

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	4
Введение	5
Развертывание коннектора	6
Установка системы Skybox Security	6
Установка коннектора "Континент-Skybox"	6
Создание учетной записи администратора для коннектора	7
Создание профиля для ЦУС в коннекторе	9
Анализ конфигурации	12
Конфигурация КШ	14

Список сокращений

АПКШ	Аппаратно-программный комплекс шифрования
ДА	Детектор атак
КШ	Криптографический шлюз
ОС	Операционная система
ПУ	Программа управления
РМ	Рабочее место
ЦУС	Центр управления сетью

Введение

Программный модуль "Коннектор "Континент-Skybox" (далее — коннектор) предназначен для выгрузки конфигурации криптографических шлюзов АПКШ "Континент" (далее — комплекс), формирования iXML-файла и его отправки на сервер Skybox Security для анализа.

Примечание. Коннектор совместим со Skybox Security версий 10 и 11.

Выгрузка и отправка конфигурации 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 (PM 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:

1. Установка системы Skybox Security и коннектора "Континент-Skybox".
2. Создание в ЦУС учетной записи администратора с ролью аудитора для коннектора.
3. Создание в коннекторе профилей для ЦУС комплекса.

Установка системы Skybox Security

Описание процесса установки системы Skybox Security приводится в руководстве по установке Skybox Security на сайте <https://downloads.skyboxsecurity.com/>.

Установка коннектора "Континент-Skybox"

Для установки коннектора "Континент-Skybox":

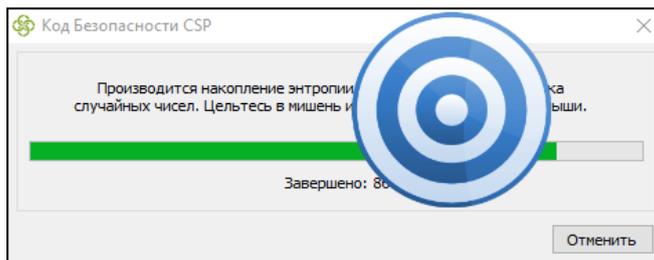
1. Запустите файл setup.exe из состава дистрибутива.
2. Установите коннектор, следуя указаниям в мастере установки.

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



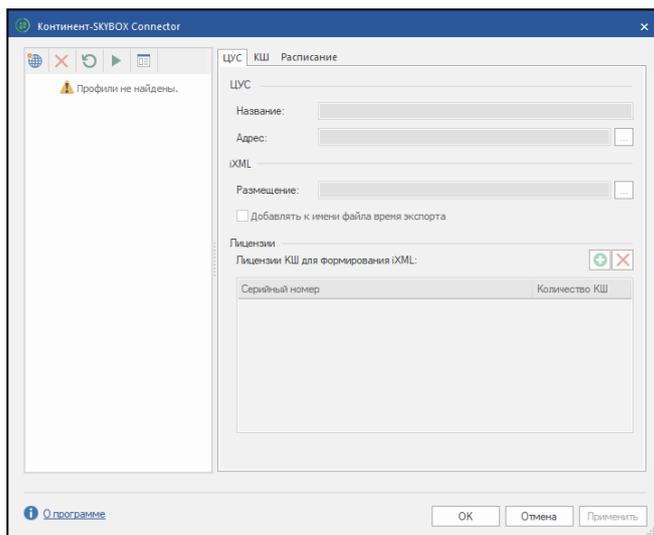
3. Запустите коннектор от имени администратора.
4. При первом запуске выполните процедуру накопления энтропии для работы датчика случайных чисел согласно появившейся на экране инструкции.

- Следуя инструкции, нажимайте на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.



Внимание! Непопадание в мишень может привести к понижению уровня накопленной энтропии и необходимости повторного выполнения данной операции.

После завершения операции накопления энтропии на экране появится окно коннектора.



Создание учетной записи администратора для коннектора

Для корректной работы коннектора необходимо создать в ПУ ЦУС учетную запись для ЦУС.

Для создания новой учетной записи:

- В ПУ ЦУС в контекстном меню объекта "Центр управления сетью | Администраторы" выберите пункт "Создать администратора...".
На экране появится окно создания администратора.
- 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.

- Нажмите кнопку "OK".
На экране появится окно ввода пароля.
- Введите пароль для шифрования ключей и нажмите кнопку "OK".
На экране отобразится окно записи ключевого носителя.
- Предъявите чистый носитель для записи ключа администратора.

6. В окне выбора носителя выберите носитель для записи ключа администратора и нажмите кнопку "ОК".

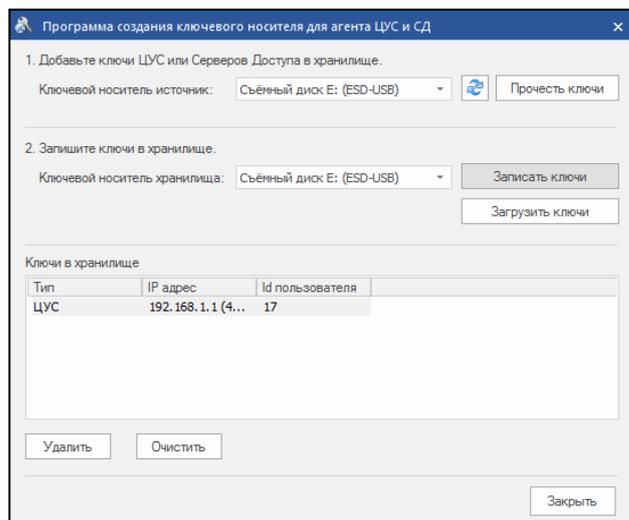
Окно создания пользователя закроется.

Далее на созданный носитель администратора коннектора необходимо записать параметры подключения к ЦУС. Для дозаписи используется программа создания ключевого носителя, входящая в состав ПУ ЦУС.

Для записи параметров подключения к ЦУС на носитель:

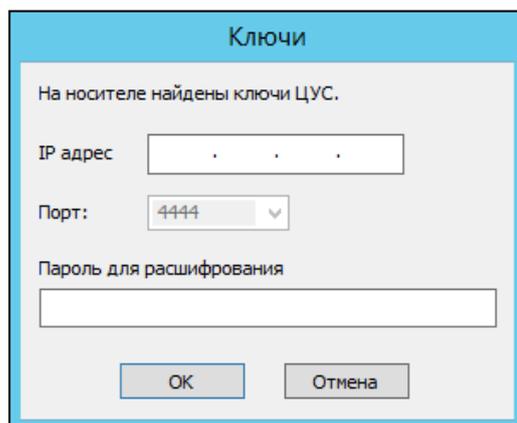
1. Подключите ключевой носитель (если он не был подключен ранее).
2. В списке объектов ПУ ЦУС выберите пункт "Центр управления сетью".
3. В панели инструментов выберите пункт "Ключевой носитель".

На экране появится окно программы создания ключевого носителя.



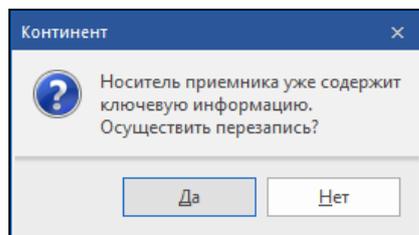
4. В раскрывающемся списке "Ключевой носитель источник" выберите ключевой носитель администратора коннектора и нажмите кнопку "Прочитать ключи".

На экране появится окно с запросом дополнительной информации.



5. Введите IP-адрес ЦУС и пароль администратора коннектора для расшифровки ключей.
6. Нажмите кнопку "ОК".
7. В раскрывающемся списке "Ключевой носитель хранилища" выберите ключевой носитель администратора коннектора, на который будут записаны ключи, и нажмите кнопку "Записать ключи".

На экране появится окно с сообщением.



8. Нажмите кнопку "Да", чтобы перезаписать ключевую информацию.
После успешного завершения записи ключевой информации на носитель список администраторов на экране дополнится соответствующей записью.

Создание профиля для ЦУС в коннекторе

После установки коннектора и создания учетной записи администратора с ролью "Аудитор" необходимо создать профиль для ЦУС в коннекторе. Для каждого ЦУС в комплексе создается отдельный ключевой носитель и отдельный профиль.

Примечание. Для корректной работы коннектора необходим сетевой доступ коннектора к ЦУС и серверу Skybox Security (для экспорта iXML-файлов конфигураций).

Для создания нового профиля для ЦУС:

1. Запустите коннектор от имени администратора.
2. Подключите к компьютеру подготовленный ключевой носитель администратора коннектора.
3. В левой части окна коннектора нажмите кнопку

На экране отобразится окно выбора адреса ЦУС.

4. Выберите из списка IP-адрес ЦУС и нажмите кнопку "ОК".
5. Выберите вкладку "ЦУС".

Значения параметров "Название" и "Адрес ЦУС" в группе "ЦУС" автоматически заполняются значениями, полученными с ключевого носителя администратора коннектора.

6. В поле "Размещение" укажите папку-хранилище (папку в памяти компьютера или папку в файловой системе Skybox Security), в которую будут сохраняться файлы конфигураций.
7. В группе "Лицензии" нажмите кнопку

В списке "Лицензии КШ для формирования iXML" появится новая строка для ввода серийного номера лицензии.

Внимание! Проверка лицензии на валидность возможна только в случае успешного подключения коннектора к ЦУС.

8. Введите серийный номер лицензии и нажмите клавишу <Enter>.

Примечание. Демо-лицензия позволяет выгружать конфигурацию с КШ, подключенных к любому ЦУС. Для одного ЦУС, независимо от количества созданных для него профилей, можно зарегистрировать только одну демо-лицензию.

9. Выберите вкладку "КШ" и нажмите кнопку
10. Отметьте в списке КШ, конфигурации которых должны быть переданы в Skybox Security, и нажмите кнопку "ОК".
Выбранные КШ отобразятся в списке на вкладке.

При необходимости установите расписание, согласно которому коннектор будет экспортировать данные.

Коннектор запускается при старте ОС Windows с помощью службы SBSservice.

В коннекторе предусмотрена возможность настройки учетной записи пользователя, от имени которой будет запускаться служба SBSservice. По умолчанию

служба коннектора запускается от имени системы (Local System), что усложняет настройку прав доступа в сетевую папку.

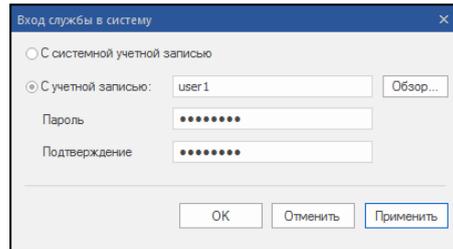
Если планируется выгрузка конфигураций в сетевую папку (например, на сервер Skybox), рекомендуется настроить запуск службы коннектора от конкретной учетной записи пользователя и выдать права на запись в сетевую папку этой учетной записи.

Для настройки запуска службы SBSERVICE от учетной записи пользователя:

1. В панели инструментов коннектора нажмите кнопку

Откроется окно настройки параметров службы.

2. В окне настройки параметров службы выберите вариант "С учетной записью".



3. Введите в текстовое поле название учетной записи или нажмите кнопку "Обзор" и в открывшемся окне выберите пользователя, от имени которого будет выполняться запуск службы SBSERVICE.

Внимание! Выбранная учетная запись должна обладать правами администратора на компьютере, на котором установлен коннектор.

4. Создайте и подтвердите пароль для пользователя.
5. Нажмите кнопку "Применить".

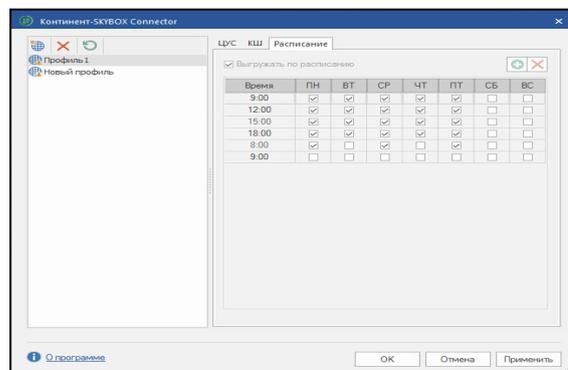
Окно настроек службы закроется.

Для запуска или остановки службы:

- для запуска службы нажмите кнопку
- для ее остановки нажмите кнопку

Для установки выгрузки конфигураций по расписанию:

1. В окне коннектора выберите вкладку "Расписание".
2. Установите отметку в поле "Выгружать по расписанию".
3. Установите или снимите отметки в таблице с днями недели и временем старта.



4. Чтобы добавить новое время старта, нажмите кнопку и в новой строке установите отметки в требуемых полях.

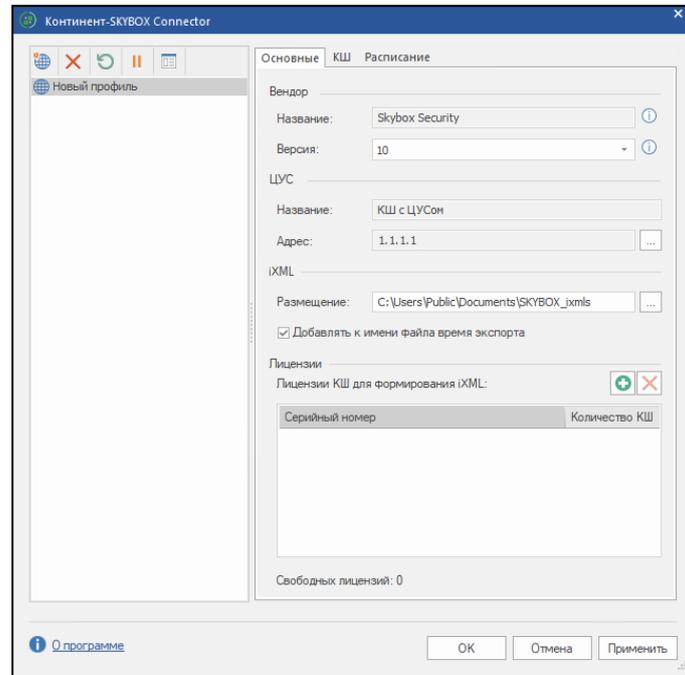
5. Нажмите кнопку "OK".

По завершении настройки расписания окно коннектора можно закрыть. Служба коннектора будет работать в фоновом режиме и выгружать конфигурации в соответствии с расписанием.

Примечание. При каждом обращении коннектора к ЦУС происходит считывание и проверка ключа администратора коннектора. На момент выгрузки по расписанию ключевой носитель администратора коннектора должен быть подключен к компьютеру, на котором установлен и запущен коннектор.

Для выгрузки конфигурации вручную:

1. В окне коннектора выберите вкладку "Основные".



2. В группе параметров "Вендор", в раскрывающемся списке "Версия" выберите версию Skybox Security, для которой предназначена выгрузка конфигурации.

3. Нажмите кнопку "Применить".

4. Выберите вкладку "КШ".

5. Выберите в списке КШ, конфигурации которых нужно экспортировать, и нажмите кнопку .

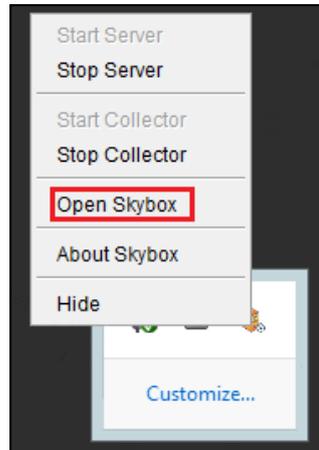
Примечание. Экспортироваться будут только КШ, на которые распространяется лицензия. Такие КШ отмечены знаком .

По завершении экспорта на экране отобразится сообщение "Экспорт успешно выполнен".

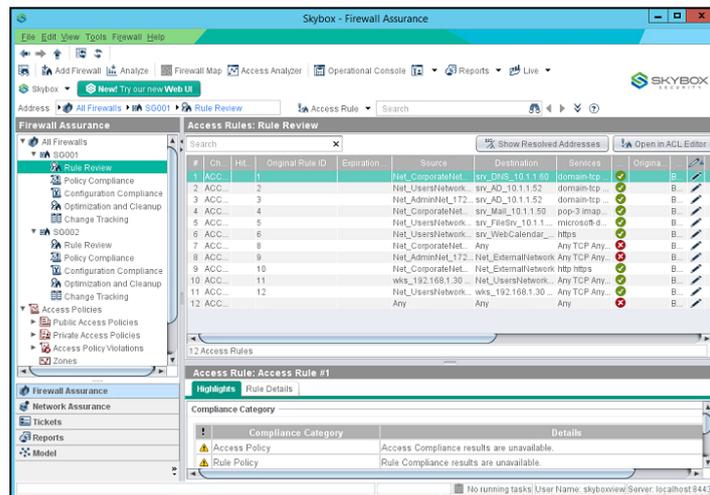
Анализ конфигурации

Для выполнения анализа конфигурации:

1. На панели задач ОС Windows выберите значок Skybox Security.
2. В контекстном меню значка Skybox Security выберите пункт "Open Skybox", чтобы открыть окно работы со службой Skybox Security.

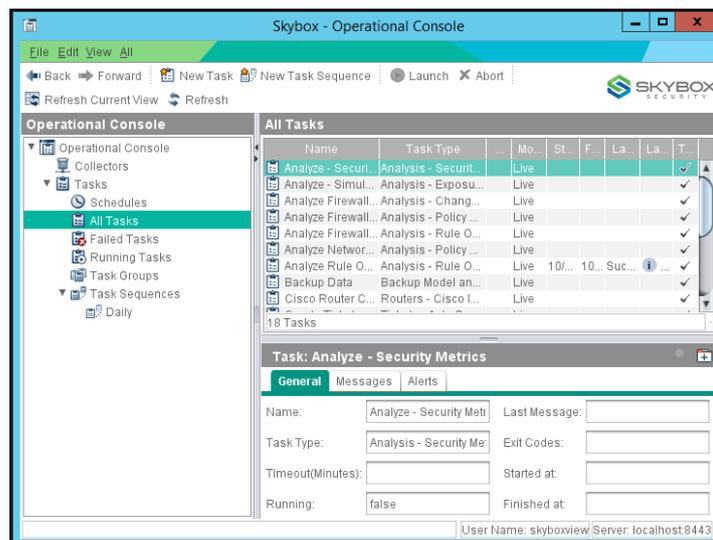


Откроется окно службы Skybox Security.



3. В панели инструментов нажмите кнопку "Operational Console".

Откроется окно "Operational Console".



4. В меню "Operational Console" выберите раздел "All Tasks".

5. В списке задач выберите задачу с типом "Import-Directory" и в контекстном меню задачи выберите пункт "Launch".

Примечание. Настройка параметров задачи описана в справочном руководстве Skybox Security Reference Guide на сайте <https://downloads.skyboxsecurity.com/>.

Служба Skybox Security приступит к выполнению задачи. Статус выполнения задачи будет отображаться в таблице задач.

6. Дождитесь выполнения задачи и вернитесь к окну "Operational Console".
7. В меню "Firewall Assurance" выберите раздел для просмотра информации о конфигурации.

Информация о конфигурации отобразится в центральной области окна.

Конфигурация КШ

В конфигурацию для анализа включаются сведения о следующих объектах в ЦУС:

- сетевые объекты и группы сетевых объектов;
- сервисы и группы сервисов;
- правила фильтрации;

Примечание. В конфигурации не учитывается контроль состояния соединения для правил фильтрации.

- правила трансляции адресов (правила NAT);
- правила ДА;
- правила статической маршрутизации.

Конфигурации КШ сохраняются в iXML-файле, каждый iXML-файл содержит конфигурацию одного объекта.

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.

По умолчанию название iXML-файла содержит имя объекта. 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.