КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент
Версия 3.7

Руководство администратора

Аутентификация пользователя

RU.88338853.501430.006 96 4 1

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

Оглавление

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.7" RU.88338853.501430.006 (далее — комплекс). В нем содержатся сведения, необходимые администратору для управления программой "Континент. Клиент аутентификации пользователя" (далее – программа).

Приступая к изучению данного руководства, необходимо предварительно ознакомиться с документом [**1**].

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru . Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training- courses/ . Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие сведения

Программа "Континент. Клиент аутентификации пользователя" предназначена для идентификации и аутентификации пользователей, зарегистрированных в комплексе.

Регистрацию пользователей выполняют средствами централизованного управления комплексом. При регистрации пользователю назначают имя и пароль.

Для успешной работы программы необходимо включение на КШ режима "Аутентификация пользователей".

Эти параметры устанавливают средствами централизованного управления комплексом [**1**]. Протокол, по которому программа и КШ обмениваются данными, см. стр.**10**.

Установка, обновление и удаление программы

Требования к программному и аппаратному обеспечению

Программа может быть установлена на любые компьютеры, программное и аппаратное обеспечение которых удовлетворяет минимальным требованиям установленной на них версии ОС Windows.

Установка программы

Для установки программы:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл setup.exe, находящийся в каталоге с дистрибутивом комплекса.

   Совет. Для установки программного обеспечения Клиента с жесткого диска скопируйте файлы с установочного диска в любой рабочий каталог (локальный или сетевой) и запустите на исполнение файл Setup.exe.

   Программа установки начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера установки.
3. Нажмите кнопку "Далее >" для продолжения установки.

   На экране появится диалог, содержащий лицензионное соглашение на использование программного продукта.
4. Прочтите лицензионное соглашение. Если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее >".

   На экране появится диалог выбора папки для размещения файлов программы.

   По умолчанию программа установки копирует файлы в каталог \Program Files \ Код Безопасности\ Аутентификация пользователя. Для установки программы в другую папку нажмите кнопку "Изменить..." и укажите нужную папку в открывшемся диалоге.
5. Нажмите кнопку "Далее >".

   На экране появится диалог "Установка".
6. Нажмите кнопку "Установить".

   Программа установки приступит к копированию файлов в указанную папку. Сообщения, появляющиеся на экране, отображают этапы процесса установки.

   По окончании процесса копирования на экране появится заключительное окно мастера установки.
7. Оставьте отметку в поле "Запустить программу", если требуется запустить программу по окончании процедуры установки, и нажмите кнопку "Готово".

   Примечание. Если запуск программы не требуется, удалите отметку из поля "Запустить программу". Позже вы сможете запустить программу вручную (см. стр.8).

   После запуска программы в системной области панели задач ОС Windows появится значок программы  . Для работы Клиента необходимо настроить параметры аутентификации (см. стр.9).

Обновление программы

Для обновления программы:

1. Выполните пп. 1–3 процедуры установки (см. стр.**6**).

   На экране появится сообщение для подтверждения запуска процедуры обновления.

2. Нажмите кнопку "Да".

   Программа начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера обновления.

3. Нажмите кнопку "Далее >" для подтверждения обновления.

   Программа приступит к обновлению версии продукта. По окончании процесса на экране появится заключительный диалог мастера установки.

4. Нажмите кнопку "Готово".

Удаление программы

Для удаления программы:

1. Нажмите кнопку "Пуск" и в главном меню ОС Windows найдите и активируйте команду "Панель управления".
2. В окне "Панель управления" активируйте элемент "Установка и удаление программ".

   Примечание. Если на компьютере установлено ПО ОС Windows Vista и выше, активируйте элемент "Программы и компоненты".

3. Выберите в списке установленных программ элемент "Континент. Аутентификация пользователя" и нажмите кнопку "Изменить".

   Примечание. В ОС Windows Vista активируйте команду "Изменить" из контекстного меню элемента.

   После выполнения подготовительных действий на экране появится стартовое окно программы удаления.

4. Нажмите кнопку "Далее >".

   На экране появится диалог для подтверждения удаления.

5. Нажмите кнопку "Удалить".

   Программа удаления приступит к удалению файлов. По завершении процесса удаления на экране появится сообщение об успешном завершении процедуры удаления.

6. Нажмите кнопку "Готово".

Работа с программой

Запуск программы вручную

Для запуска программы вручную:

- Нажмите кнопку "Пуск" ("Start") и выберите в главном меню ОС Windows команду "Программы> Код Безопасности> Континент. Аутентификация пользователя".

  Программа будет запущена. В системной области панели задач ОС Windows появится значок программы (см. Табл.1 на стр.**8**).

Меню управления параметрами

Управление параметрами программы выполняют из специального меню.

Для вызова меню:

- Наведите указатель мыши на значок программы, расположенный в системной области панели задач ОС Windows, и нажмите правую кнопку мыши.

  На экране появится меню.

Табл.1 Значок программы аутентификации

Значок	Описание
	Устанавливается соединение с КШ
	Соединение с КШ установлено
	Соединение с КШ отсутствует

Табл.2 Команды меню управления программой аутентификации

Команда	Описание
Подключить...	Запускает процедуру установки соединения с КШ в соответствии со значениями параметров, указанных в диалоге "Параметры аутентификации"
Отключить	Разрывает соединение с КШ
Параметры...	Открывает диалог "Параметры аутентификации" для настройки программы
Журнал приложений системы	Вызывает на экран окно "Просмотр событий" ОС Windows
О программе	Вызывает на экран окно с информацией о версии продукта и авторских правах
Выход	Завершает работу программы и удаляет значок из системной области панели задач

Подключение к КШ

Подключение выполняется в соответствии со значениями параметров, указанных в диалоге "Параметры аутентификации" (см. стр.**9**).

Для подключения к КШ:

1. Вызовите контекстное меню значка программы (см.стр.**8**).
2. Выберите команду "Подключить...".

   На экране появится запрос пароля.

> **Примечание.** Запрос появляется только при отсутствии отметки в поле "Запомнить пароль" диалога "Параметры аутентификации".

3. Укажите нужное имя и пароль и нажмите кнопку "ОК".

Для отключения от КШ используйте команду контекстного меню "Отключить".

Настройка параметров аутентификации

Для настройки параметров:

1. Вызовите контекстное меню значка программы (см.стр.8).
2. Выберите команду "Параметры...".

   На экране появится диалог "Параметры аутентификации".
3. Заполните поля диалога и нажмите кнопку "ОК".

Логин	Имя пользователя, зарегистрированное в комплексе
Пароль	Пароль пользователя, назначенный при регистрации
Запомнить пароль	При наличии отметки запрос на пароль при подключении к КШ не выводится
Адрес	Внутренний IP-адрес КШ, в защищенной сети которого работает пользователь
Время ожидания соединения, сек.	Период ожидания (в секундах), по истечении которого при отсутствии ответа от КШ соединение будет признано неудавшимся
Запускать программу после загрузки системы	При наличии отметки программа запускается автоматически после загрузки системы

Просмотр событий

События, относящиеся к программе, сохраняются в журнале событий и доступны для просмотра.

Для просмотра информации о событии:

1. Вызовите контекстное меню значка программы (см.стр.8).
2. Активируйте команду "Журнал приложения системы".

   На экране появится окно журнала событий ОС Windows.

   Каждая запись в журнале содержит дату, время и информацию о событии.

Приложение

Протоколы и порты

В данном разделе представлены сведения о протоколах и портах, используемых для связи между компонентами комплекса.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса по протоколам и портам, указанным в таблице.

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/443	Обмен сообщениями между СД и АП. При включенном на АП режиме защищенного соединения "Потоковое подключение (TCP)" или "Подключение через прокси-сервер"	АП / СД. СД / АП	АПКШ "Континент" 3.7
TCP/4431, 1025-65535	Обмен сообщениями между СД и ПУ СД. Обмен сообщениями между агентом ЦУС и СД и СД. ПУ СД и агент ЦУС и СД устанавливают подключение со случайного порта из диапазона 1025-65535 к СД на порт 4431. СД отвечает с порта 4431 на тот порт компьютера с ПУ СД или с агентом ЦУС и СД, с которого пришло подключение	ПУ СД / СД. СД / ПУ СД. Агент ЦУС и СД /СД. СД / агент ЦУС и СД	АПКШ "Континент" 3.2.21 и более поздние версии
TCP/4444	Передача сообщений от ПУ ЦУС к ЦУС; обмен сообщениями между ЦУС и агентом ЦУС; обмен сообщениями между агентом обновлений БРП и ЦУС. ПУ ЦУС, агент ЦУС и СД, агент обновлений БРП, агент РКН устанавливают подключение со случайного порта 1024-65535 на порт ЦУС 4444. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. Агент ЦУС и СД / ЦУС. ЦУС / агент ЦУС и СД. Агент обновлений БРП / ЦУС	
TCP/4445	Передача обновлений ПО от ПУ ЦУС к ЦУС и обмен сообщениями между ПУ ЦУС и агентом ЦУС. ПУ ЦУС устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4445. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. ПУ ЦУС / агент ЦУС и СД. Агент ЦУС и СД / ПУ ЦУС	АПКШ "Континент" 3.1.18 и более поздние версии

Протокол/ порт	Описание	Источник/получатель	Примечание
TCP/4446	Аутентификация пользователей в защищенном сегменте сети. Клиент аутентификации устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4446. ЦУС отвечает на тот порт, с которого было обращение	Компьютер с установленной программой "Клиент аутентификации пользователя" / СУ	АПКШ "Континент" 3.6 и более поздние версии
TCP/5100	Передача сообщений от ЦУС к СУ и обмен сообщениями между СУ в кластере. Узел кластера обращается к парному с порта 10000-65535 на порт 5100. Парный отвечает на тот порт, с которого было обращение	ЦУС / СУ. Основное СУ / резервное СУ. Резервное СУ / основное СУ	АПКШ "Континент" 3.0 и более поздние версии
TCP/5101	Передача сообщений от СУ к ЦУС. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5101. ЦУС отвечает на тот порт, с которого было обращение	СУ / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
TCP/5102	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5102. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / СУ	АПКШ "Континент" версии 3.5
TCP/5103	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5103. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / СУ	АПКШ "Континент" 3.6 и более поздние версии
UDP/5101	Передача сообщений от СУ к ЦУС. Узел обращается с порта 5100 на порт ЦУС 5101. ЦУС отвечает с порта 5101 на порт 5100	СУ (исходящий порт 5100) / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
UDP/5106 UDP/5107	Поддержка работы СУ за NAT. В зависимости от используемых классов трафика, узлы отправляют пакеты с портов 10000-10031 на порты ЦУС 5106-5107	СУ / ЦУС	АПКШ "Континент" 3.6 и более поздние версии

Протокол/ порт	Описание	Источник/получатель	Примечание
UDP/5557	Передача сообщений об активности между СУ в кластере. Узлы кластера обмениваются пакетами с порта 5557 на порт 5557	Основное СУ / резервное СУ. Резервное СУ / основное СУ	АПКШ "Континент" 3.0 и более поздние версии
UDP/4433	Обмен сообщениями между СД и АП. Номер порта по умолчанию; изменяется в программе управления СД	АП / сервер доступа	АПКШ "Континент" 3.2.21 и более поздние версии
UDP/7500	Обмен сообщениями между СД и АП. Номер порта по умолчанию; изменяется в настройках виртуального адаптера Continent 3 PPP Adapter	Сервер доступа / АП	АПКШ "Континент" 3.2.21 и более поздние версии
UDP/10000	Передача зашифрованного трафика. Узлы обмениваются пакетами с порта 10000 на порт 10000	СУ / СУ. СУ / ЦУС	АПКШ "Континент" 3.5
UDP/10000-10031	Передача зашифрованного трафика. В зависимости от используемых классов трафика, узлы обмениваются пакетами с портов 10000-31 на соответствующие порты 10000-31	СУ / СУ. СУ / ЦУС	АПКШ "Континент" 3.6 и более поздние версии

Документация

1.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Централизованное управление комплексом
2.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами
3.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит
4.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя
5.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Сервер доступа
6.	Аппаратно-программный комплекс шифрования "Континент". Руководство пользователя. Программа мониторинга КШ
7.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Тестирование каналов связи
8.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Обновление программного обеспечения
9.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Автоматизированное рабочее место генерации ключей
10.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Система обнаружения вторжений

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.