

## **Средство криптографической защиты информации**

### **"Континент-АП"**

#### **Версия 4**

#### **Комментарии к релизу 4.1.680.0**

Документ содержит описание возможностей изделия "Средство криптографической защиты информации "Континент-АП". Версия 4" (далее — СКЗИ "Континент-АП", "Континент-АП") релиза 4.1.680.0, а также особенностей и ограничений, которые необходимо учитывать при его эксплуатации.

## **Оглавление**

<b>1.</b>	<b>Изменения и новые возможности .....</b>	<b>2</b>
<b>2.</b>	<b>Ограничения на поддержку аппаратных и программных средств .....</b>	<b>3</b>
<b>3.</b>	<b>Особенности работы и ограничения .....</b>	<b>4</b>

## **1. Изменения и новые возможности**

- 1.** Модульная архитектура, при которой реализация криптографических алгоритмов выполняется в отдельном стороннем программном модуле — криптопровайдере.
- 2.** Регистрация событий с самодостаточным текстовым описанием в журнале приложений ОС Windows и лог-файлах.
- 3.** Возможность сбора диагностической информации.
- 4.** Регистрация рабочего места СКЗИ.
- 5.** Пользовательский интерфейс с настраиваемыми цветовыми схемами.
- 6.** Автоматическое скачивание CRL.
- 7.** Автоматическое определение CDP из сертификатов для обновления списков CRL.
- 8.** Создание подключения по двум типам протокола, версии 3.X (подключение к серверу доступа) и 4.X (подключение к узлу безопасности).
- 9.** Автоподключение к серверу доступа (СД) или узлу безопасности (УБ) после старта системы с профилем по умолчанию.
- 10.** Создание профилей подключения к УБ (по протоколу 4.X).
- 11.** Импорт профиля, созданного по протоколу 4.X.
- 12.** Автоматическое переподключение при разрыве соединения (5 попыток).
- 13.** Два вида аутентификации при подключении по протоколу 4.X (по сертификату пользователя и по логину/паролю).
- 14.** Автоматическое определение настроек системного прокси.
- 15.** Облегченная процедура установки ПО с помощью одного окна, требующая минимального участия пользователя.
- 16.** Быстрый старт "Континент-АП". Возможность импорта конфигурационного файла и автоматического установления подключения.
- 17.** Возможность подключения к СД/УБ до входа пользователя в систему с помощью настроенного глобального профиля.
- 18.** Экспорт настроек конфигурации.
- 19.** Два режима настройки работы "Континент-АП" — автоматический (импорт конфигурационного файла, содержащего все необходимые настройки) и ручной.

## 2. Ограничения на поддержку аппаратных и программных средств

1	Ключевое устройство	<ul style="list-style-type: none"><li>• USB-флеш-накопитель;</li><li>• токены и смарт-карты: Рутокен S, Рутокен Lite, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Flash, JaCarta PKI, JaCarta PKI/ГОСТ, JaCarta ГОСТ; JaCarta 2 ГОСТ;</li><li>• идентификаторы DS1995, DS1996</li></ul>
2	Операционная система	<ul style="list-style-type: none"><li>• Windows Server 2016 x64;</li><li>• Windows Server 2012 R2 x64;</li><li>• Windows Server 2012 x64;</li><li>• Windows 10 x86/x64;</li><li>• Windows 8.1 x86/x64;</li><li>• Windows 7 SP1 x86/x64</li></ul>
3	Криптопровайдер	Код Безопасности CSP 4.0.640.0 КриптоПро CSP 4.0 (R3, R4); 5.0

### 3. Особенности работы и ограничения

1. Для корректного импорта сертификатов с привязкой к ключевому контейнеру необходимо чтобы у пользователя, производящего импорт, были права, разрешающие запись и/или изменения ветки реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY\Keys` `HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MY\Keys`.
2. Если при подключении к СД 3.7 появляется сообщение "Не найден корневой сертификат", необходимо проверить следующее:
  - Установлен ли на машине с "Континент-АП" корневой сертификат, удостоверяющий пользовательский сертификат.
  - Установлен ли на машине с "Континент-АП" корневой сертификат, удостоверяющий сертификат сервера.
  - Имеется ли в базе сервера доступа, к которому осуществляется подключение, пользовательский сертификат.
3. Для исправления ошибки подключения с ненастроенным профилем от версии "Континент-АП" 3.7.7 после обновления необходимо:
  - Перейти в папку `C:\Users\admin\AppData\Roaming\ContinentVPNClient`.
  - Открыть при помощи любого редактора (например, WordPad) файл `UserConfig.json`.
  - Найти блок настроек необходимого подключения.
  - В параметре `"useCertificate"` изменить значение с `"false"` на `"true"`.
4. Для корректной установки "Континент-АП" на компьютер с предустановленным антивирусом Avast Free необходимо на время установки программы в настройках антивируса включить режим повышенной безопасности и во время установки добавлять "Континент-АП" в исключения всякий раз, когда будет возникать предупреждение о блокировке устанавливаемой программы, или отключить на время установки проверку антивируса вообще.
5. Для изменения настроек CRL и профиля подключения "Континент-АП" необходимо запускать программу от имени администратора. Исключение составляет Win 2016 srv — пользователь с правами администратора имеет доступ к настройкам сразу.
6. Если на компьютер предварительно были установлены "КриптоПро CSP" и TLS-клиент версии 2.0, то при установке "Континент-АП" "Код Безопасности CSP" установлен не будет. Наличие отметки о возможности совместной работы со сторонним криптопровайдером в процессе установки будет проигнорировано.
7. Если во время обновления было установлено соединение с сервером доступа и после перезагрузки "Континент-АП" не запускается, а также появляется сообщение об ошибке "Указанная служба не установлена", то необходимо произвести восстановление ПО из msi-пакета с диска с установочными файлами или воспользоваться утилитой восстановления через меню "Пуск".
8. Если установка "Континент-АП" производится пользователем, имеющим ограниченные права, то после перезапуска системы в конце установки, программа самостоятельно не стартует и набор энтропии не производится. Для дальнейшей работы необходимо вручную запустить программу двойным кликом по ярлыку на рабочем столе, или из меню "Пуск".
9. Если установка производилась пользователем с правами администратора, то программа после перезапуска системы стартует автоматически и на экране появляется мишень для первоначального набора энтропии.
10. Для проброса всех соединений через VPN на сервере доступа задаются соответствующие правила фильтрации. Для того чтобы весь трафик на компьютере с "Континент-АП" при установленном подключении проходил через сервер доступа, необходимо чтобы в системе отсутствовал маршрут с метрикой меньше "276". Если такой имеется, то необходимо либо вручную увеличить метрику для сетевого подключения, либо удалить данный маршрут.
11. "Континент-АП" 4 не совместим с Агентом БРП версий 3.7 и 3.9.
12. Для использования персональных ключевых носителей Рутокен и JaCarta, необходимо скачать и установить их драйверы.
13. Криптопровайдер "КриптоПро CSP" позволяет импортировать сертификаты только собственного выпуска. Криптопровайдер "Код безопасности CSP" позволяет производить импорт сертификатов, выпущенных как посредством ПО "Код безопасности CSP", так и ПО "КриптоПро CSP" (сертификаты, соответствующие ГОСТ Р 34.10-2001).
14. После обновления криптопровайдера необходима перезагрузка компьютера.
15. Не допускается присутствие в системе ключевых контейнеров с одинаковыми именами.

- 16.** При использовании на "Континент-АП" сертификатов, выпущенных в ПУ СД/УБ на криптопровайдере "КриптоПро CSP", необходимо в настройках ПО отключать проверку сертификатов по CRL. В противном случае подключение к СД/УБ будет невозможно.
- 17.** При изменении адреса DNS-сервера в системе изменение будет учтено в настройках "Континент-АП" только после перезапуска приложения.
- 18.** Если в "Континент-АП" выбрана опция автоматической настройки прокси, то при изменении настроек прокси-сервера в системе необходимо перезапустить приложение, чтобы изменения вступили в силу.
- 19.** При совместной работе "Континент-АП" с Secret Net Studio (SNS) при настройках полномочного режима и конфиденциального доступа в SNS не рекомендуется включать запрет доступа к каталогу public\continentvnpclient. В противном случае работа АП будет невозможна.
- 20.** "Континент-АП" не предназначен для использования в режиме шлюза, пропускающего весь объем трафика.
- 21.** "Континент-АП" поддерживает работу только с ключами, созданными с использованием параметров 1.2.643.2.2.35.1, 1.2.643.2.2.35.2, 1.2.643.2.2.35.3, 1.2.643.2.2.36.0, 1.2.643.2.2.36.1. Для проверки валидности сертификата откройте диалог просмотра свойства сертификата. Перейдите на вкладку "Состав" и выберите поле "Параметры открытого ключа". Убедитесь, что восьмой и девятый байты слева имеют значение "02". Если значение не совпадает, создайте запрос на другой сертификат или получите новый сертификат из внешних источников.
- 22.** Если "Континент-АП" версии 4 устанавливается на компьютер, на котором ранее была установлена версия 3.7.7.651, может возникнуть ошибка при создании запроса на создание сертификата с включенной опцией "Подготовить бланк запроса на сертификат". Для исправления ошибки зайдите в ветку реестра HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType0\CryptDLLFindOIDInfo и удалите папку 1.2.643.2.1.3.1.2.1.
- 23.** Если на компьютер установлена англоязычная версия "Континент-АП", с англоязычной ОС, пользователь может получать русскоязычные сообщения от СД 3.7 или СД 3.9. Данные сообщения не планируется переводить на английский язык. Чтобы прочитать их на русском, необходимо в настройках ОС Windows добавить поддержку русского языка для программ Unicode.
- 24.** Если при создании запроса на сертификат была выбрана версия протокола 4.X, в поле "Адрес" необходимо указывать то же значение, которое указано в поле CommonName сертификата сервера (имя должно быть написано латиницей без пробелов и представлять собой DNS-имя или IP-адрес сервера). В противном случае подключение не будет установлено, а на экране появится сообщение "Адрес сервера доступа не соответствует имени, на которое выдан сертификат сервера". Для устранения ошибки проверьте правильность заполнения полей. Если поле CommonName сертификата сервера содержит русские буквы и/или пробелы, перевыпустите сертификат с корректными параметрами значения.
- 25.** При обновлении "Континент-АП" с версии 3.7 до версии 4.1 настройки прокси автоматически перенесены не будут. Их необходимо самостоятельно сохранить заранее.
- 26.** Особенности подключения до логона. "Континент-АП" позволяет устанавливать соединение с СД/УБ до входа в систему с помощью глобального профиля. Для активирования этого способа нужно выбрать в меню настроек пункт "Основные", раздел "Режим запуска", и установить отметку в поле "Разрешить использования подключения до логона"(по умолчанию опция отключена). Для проверки активирования нужно выполнить выход из системы. На экране выбора пользователя в правом нижнем углу должна появиться кнопка "Вход в сеть" (значок в виде двух мониторов). Для подключения нажмите кнопку "Вход в сеть и после установления соединения войдите в домен под учетной записью пользователя.
- 27.** Активирование настройки "Разрешить подключение до логона" приводит к более медленному, чем обычно, входу пользователя в систему.
- 28.** Автоматическое подключение с профилем по умолчанию не может быть установлено, если по каким-то причинам, пользователь прекратил работу, не разорвав соединение. В таком случае при попытке подключения на экране появится сообщение — "Автоматическое подключение с профилем по умолчанию не будет производиться, если ранее было установлено другое подключение". Разорвите установленное соединение и запустите "Континент-АП" заново.
- 29.** Период действия закрытого ключа сертификата по умолчанию составляет 1 год и 3 месяца от даты начала срока действия сертификата. После истечения данного периода работа с сертификатом будет невозможна. Рекомендуется перевыпустить сертификат.
- 30.** При установке "Континент-АП" на компьютер, на котором используется англоязычная версия SNS 8.4 или 8.5, криптопровайдер "Код безопасности CSP" перезаписывает значение в ветке

реестра HKEY\_LOCAL\_MACHINE\SOFTWARE\Security Code\Secret Net Studio\ProductLocale (меняет его на ru-RU), что может привести к ошибке установки. Чтобы решить проблему:

- исправьте значение в указанной ветке реестра на en-EN;
- установите дополнительные библиотеки в реестр для исправления ошибки. Получить необходимые библиотеки и инструкцию по их установке можно в Службе технической поддержки компании "Код Безопасности".

**Компания "Код Безопасности"**

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	8 495 982-30-20
Факс:	8 495 744-29-31
E-mail:	info@securitycode.ru
Web:	<a href="https://www.securitycode.ru">https://www.securitycode.ru</a>