КОД безопасности

Средство криптографической защиты информации

Континент-АП

Версия 4 (исполнение 9)

Руководство администратора

iOS и iPadOS

RU.АМБС.58.29.12.007 91

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

АП	Абонентский пункт
АПКШ	Аппаратно-программный комплекс шифрования
ОС	Операционная система
СД	Сервер доступа
СКЗИ	Средство криптографической защиты информации
CRL	Certificate Revocation List
DNS	Domain Name System
IP	Internet Protocol
MTU	Maximum Transmission Unit
NTLM	NT LAN Manager
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Введение

Документ предназначен для администраторов изделия "Средство криптографической защиты информации "Континент-АП". Версия 4 (исполнение 9)" RU.АМБС.58.29.12.007. В нем содержатся сведения, необходимые для настройки и эксплуатации СКЗИ "Континент-АП" на платформе ОС iOS и iPadOS.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-800-505-30-20 или по электронной почте support@securitycode.ru.

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 https://www.securitycode.ru/company/education/training-courses/.

Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1
Общие сведения

Назначение абонентского пункта

СКЗИ "Континент-АП" предназначено для установления защищенного соединения и обмена зашифрованными данными через общедоступные сети с СД изделий "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7" RU.88338853.501430.006, "Аппаратно- программный комплекс шифрования "Континент". Версия 3.9" RU.88338853.501430.022 (далее — АПКШ "Континент") и узлом безопасности с включенным компонентом "Сервер доступа" изделия "Континент. Версия 4" RU.АМБС.58.29.12.001.

Программное обеспечение абонентского пункта реализовано в виде приложения "Континент-АП". Приложение устанавливается на мобильные устройства, функционирующие под управлением iOS и iPadOS от версии 10.0 до версии 13.x.

Абонентский пункт реализует следующие основные функции:

- установление защищенного соединения и обмен зашифрованными данными с сервером доступа АПКШ "Континент";
- контроль целостности программного обеспечения "Континент-АП";
- автоматическая регистрация событий, связанных с функционированием "Континент-АП".

Поддерживаемые мобильным устройством сетевые интерфейсы:

- подключение через беспроводные сети Wi-Fi (802.11 a/b/g/n);
- подключение через беспроводные сети GPRS/3G/4G.

"Континент-АП" имеет следующие технические характеристики:

- алгоритм шифрования — соответствует ГОСТ 28147-89, длина ключа 256 бит;
- защита передаваемых данных от искажения — соответствует ГОСТ 28147-89 в режиме выработки имитовставки.

Сертификаты

Для создания защищенного соединения между "Континент-АП" и сервером доступа пользователь "Континент-АП" получает у администратора безопасности и устанавливает на своем мобильном устройстве следующие сертификаты:

- сертификат пользователя абонентского пункта;
- корневой сертификат, удостоверяющий сертификат пользователя.

В зависимости от указаний администратора пользователь "Континент-АП" получает сертификаты двумя способами:

- Администратор безопасности передает пользователю "Континент-АП" корневой и пользовательский сертификаты вместе с закрытым ключом пользователя, записанным на карте памяти или внешнем носителе.
- По требованию администратора безопасности пользователь "Континент-АП" создает на своем мобильном устройстве запрос на получение сертификата пользователя.

> **Примечание.** Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи. Передача файлов сертификатов должна выполняться по защищенным каналам связи.

Второй способ является предпочтительным, так как позволяет пользователю сохранить в тайне ключевой контейнер и пароль. Кроме того, при создании запроса на сертификат пользователь самостоятельно указывает информацию о себе, что обеспечивает максимальную точность данных.

Профили

Чтобы установить соединение с СД, необходимо выполнить настройку параметров подключения. Так как параметры подключения изменяются (например, подключение к разным СД, использование разных сертификатов и т. д.), для каждого подключения предварительно устанавливаются конкретные значения параметров и сохраняются в виде профиля настроек с присвоенным ему именем. Назначение параметров подключения приведено в таблице ниже:

Имя профиля
Название профиля для подключения к СД
Версия сервера доступа
Номер версии СД, к которому будет подключаться пользователь. Версия СД заполняется автоматически. Если был выбран пользовательский сертификат для СД версии 3.x, версию СД можно изменить на 4
Сервер доступа
IP-адрес или имя сервера доступа
Режим защищенного соединения
Способ подключения абонентского пункта к СД. Может принимать значения: • стандартное подключение (TCP); • потоковое подключение (UDP); • подключение через прокси (только для TCP). Значение по умолчанию — TCP. Для СД 3.x можно установить значение "UDP". Для СД 4.x режим защищенного соединения всегда TCP
Прокси-сервер
При нажатии на строку параметра открывается окно настроек подключения к прокси-серверу (см. ниже). Хранит имя или IP-адрес прокси-сервера. Доступен только при режиме защищенного соединения через TCP
Адрес
Сетевое имя или IP-адрес прокси-сервера
Порт
Порт прокси-сервера. Значение по умолчанию — 3128
Аутентификация
Позволяет выбрать тип аутентификации на прокси-сервере. Может принимать значения: • без аутентификации; • Basic; • NTML
Имя пользователя
Имя пользователя для аутентификации на прокси-сервере
Пароль
Пароль пользователя для аутентификации на прокси-сервере
Сертификат
При нажатии на строку параметра открывается окно выбора сертификатов, необходимых для подключения к СД. Список доступных сертификатов представляет собой список импортированных сертификатов
Использовать прокси-сервер
Отвечает за использование прокси-сервера. Может принимать значения: • "ВКЛ" — использовать прокси-сервер; • "ВЫКЛ" — не использовать прокси-сервер

Аутентификация по сертификату
Позволяет управлять аутентификацией с использованием сертификата и ключевого контейнера. Может принимать значения: • "ВКЛ" — запрашивать пароль от ключевого контейнера; • "ВЫКЛ" — запрашивать учетные данные пользователя (логин и пароль)
Сохранить пароль
Позволяет сохранить пароль для подключения к СД
Дополнительные настройки
При активации делает доступными для управления следующие параметры: • порт сервера доступа; • порт клиента; • основной DNS-сервер; • альтернативный DNS-сервер; • домен; • MTU
Порт сервера доступа
Значения по умолчанию: • для TCP — 443; • для UDP — 4433
Порт клиента
Порт мобильного устройства. Значение по умолчанию — 7500
Основной DNS-сервер **Альтернативный DNS-сервер**
По умолчанию используются адреса DNS-серверов, получаемые от СД. Если адреса от СД не поступают, их указывают вручную. Адреса, полученные от СД, имеют приоритет над адресами, указанными вручную
Домен
При необходимости можно указать DNS-суффикс, добавляемый автоматически к имени хоста при обращении к защищаемым ресурсам. По умолчанию не используется
MTU
Максимальный размер блока (в байтах) на канальном уровне сети. Значение по умолчанию — 1500

Реализована возможность редактирования списка профилей: добавление, удаление и редактирование параметров выбранного профиля.

Для использования профиля при подключении к СД необходимо сделать его активным. Активным может быть только профиль с привязанным сертификатом. При подключении активный профиль используется по умолчанию.

Настройки

Перед установлением соединения с СД необходимо настроить общие параметры, действующие для всех подключений. Назначение общих настроек подключения разъясняется в таблице ниже:

Постоянное соединение
Соединение, отключаемое только средствами настройки общих параметров подключения, автоматически восстанавливается после потери сетевого соединения. Для реализации постоянного соединения с сервером доступа предварительно настройте или активируйте профиль подключения. Может принимать значения: • "ВКЛ"; • "ВЫКЛ". Применение параметра делает невозможным управление некоторыми другими параметрами подключения (см. ниже). Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Переподключение"; • "Соединение по запросу"
Переподключение
Автоматическое переподключение при потере сетевого соединения или при разрыве защищенного канала по инициативе сервера доступа АПКШ "Континент". Может принимать значения: • "ВКЛ"; • "ВЫКЛ". Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Постоянное соединение"; • "Соединение по запросу"
Количество попыток переподключения
Значение по умолчанию — 3. После последней неудачной попытки выводится сообщение об ошибке подключения. Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Постоянное соединение"; • "Соединение по запросу"
Время ожидания переподключения, с
Пауза между попытками подключения (в секундах). Значение по умолчанию — 30. Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Постоянное соединение"; • "Соединение по запросу"
Время ожидания при бездействии, с
Время неактивности (в секундах), по истечении которого произойдет отключение от СД. Под неактивностью понимается отсутствие трафика в защищенном канале. Значение по умолчанию — 600. Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Постоянное соединение"; • "Соединение по запросу"

Соединение по запросу
Может принимать значения: • "ВКЛ"; • "ВЫКЛ". Значение по умолчанию — "ВЫКЛ". При активации параметра на экране появляется уведомление о необходимости выполнения тестового подключения. Это нужно для того, чтобы АП получил список защищенных ресурсов от СД, как только пользователь выполнит аутентификацию. При попытке пользователя получить доступ к защищенному ресурсу — АП автоматически установит соединение с СД с использованием активного профиля. Если пароль ключевого контейнера или учетные данные (логин и пароль) не были сохранены ранее, при подключении к СД пользователь получит уведомление о необходимости перехода в приложение для выполнения аутентификации. Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Постоянное соединение"; • "Переподключение"
Максимальное время бездействия, с
Время неактивности (в секундах), по истечении которого произойдет отключение от СД, если активирован параметр "Соединение по запросу". Под неактивностью понимается отсутствие трафика в защищенном канале. Значение по умолчанию — 120. Недоступно для управления, если активирован хотя бы один из следующих параметров: • "Постоянное соединение"; • "Соединение по запросу"
Проверка по CRL
Позволяет управлять функцией проверки актуальности сертификата по списку отозванных сертификатов. Может принимать значения: • "ВКЛ"; • "ВЫКЛ"
Журнал
Позволяет настроить уровень детализации журнала "Континент-АП" (см. стр. **29**). Может принимать значения: • Базовый; • Расширенный
Отправлять отчеты об ошибках в Код Безопасности
Может принимать значения: • "ВКЛ"; • "ВЫКЛ". При активации параметра приложение "Континент-АП" автоматически отправляет отладочный журнал и отчеты об ошибках на серверы компании "Код Безопасности"

Предусмотрены операции импорта конфигурации, экспорта и импорта настроек. Операция экспорта применяется при переносе всех настроек приложения, настроенного на конкретном мобильном устройстве, на другое устройство с установленным "Континент-АП". Операция импорта настроек применяется для загрузки на конкретное устройство настроек приложения, экспортированных с другого устройства с установленным "Континент-АП".

Глава 2
Ввод в эксплуатацию

Установка и первый запуск приложения

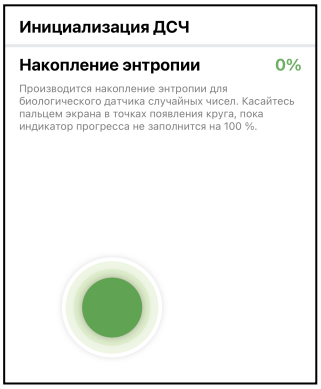
Установка приложения "Континент-АП" выполняется пользователем из магазина приложений "App Store".

Внимание! Для работы с App Store необходимо наличие Apple ID.

Для установки и первого запуска приложения:

1. В магазине "App Store" найдите приложение "Континент-АП" и загрузите его на свое устройство.
2. Запустите "Континент-АП".

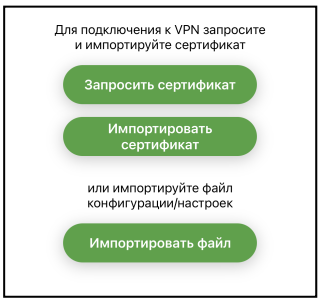
   На экране появится сообщение с инструкцией и индикатором накопления энтропии для биологического датчика случайных чисел.



3. Нажимайте на зеленый круг на экране.

   Примечание. Накопление энтропии используется для создания фиктивного ключевого контейнера. Ключевой контейнер требуется для подключения по анонимному TLS с использованием самоподписанного корневого сертификата. При удалении всех данных приложения и через год с момента последнего накопления энтропии пользователь должен заново накопить энтропию при первом запуске приложения.

   Когда индикатор накопления энтропии заполнится на 100 %, откроется окно загрузки "Континент-АП".



Внимание! В начале работы "Континент-АП" появится запрос на создание VPN-конфигурации, которая необходима для корректной работы приложения. VPN-конфигурация создается автоматически после подтверждения в окне запроса. Создание VPN-конфигурации может занять несколько минут. Если сразу после установки и настройки "Континент-АП" не удается установить соединение с СД, возможно, VPN-конфигурация еще не создалась. Для просмотра сведений о VPN-конфигурации выберите "Настройки" > "Основные" > "VPN" > "VPN Continent".

Настройка приложения

Для создания защищенного соединения между "Континент-АП" и сервером доступа (далее — СД) пользователь "Континент-АП" получает у администратора безопасности и устанавливает на своем мобильном устройстве следующие сертификаты:

- сертификат пользователя абонентского пункта;
- корневой сертификат, удостоверяющий сертификат пользователя.

В зависимости от указаний администратора пользователь настраивает приложение двумя способами:

- администратор безопасности передает пользователю "Континент-АП" файл конфигурации, пользователь выполняет импорт полученной конфигурации (см. стр. **26**);
- по требованию администратора безопасности пользователь "Континент-АП" создает на своем мобильном устройстве запрос на сертификат пользователя (см. стр. **21**). Администратор безопасности передает пользователю корневой и пользовательский сертификаты, записанные на внешнем носителе. Пользователь выполняет импорт полученных сертификатов на экране загрузки (см. стр. **11**) и настройку параметров профиля (см. стр. **7**).

> **Примечание.** Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи. Передача файлов сертификатов должна выполняться по защищенным каналам связи.

Второй способ является предпочтительным, так как позволяет пользователю сохранить в тайне ключевой контейнер и пароль. Кроме того, при создании запроса на сертификат пользователь самостоятельно указывает информацию о себе, что обеспечивает максимальную точность данных.

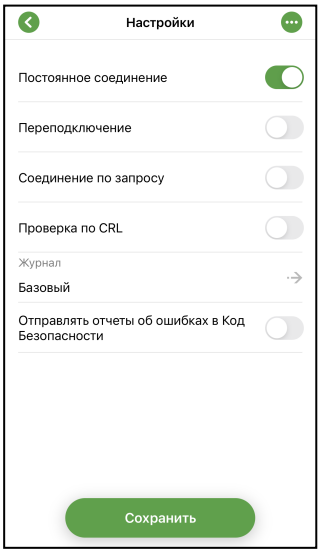
Подключение к серверу доступа

Перед подключением к СД необходимо настроить общие параметры подключения.

Для настройки общих параметров подключения:

1. Вызовите меню главного окна приложения (см. стр. **15**) и нажмите "Настройки".

   На экране появится окно настройки общих параметров подключения.



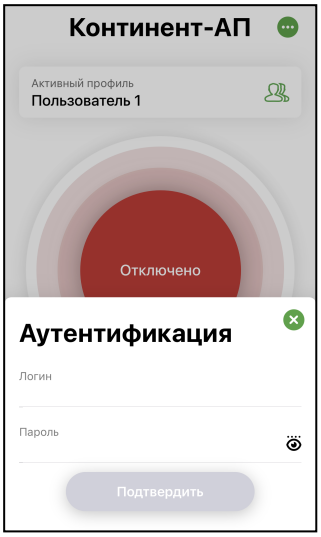
2. Установите значения параметров (см. стр. **9**) и нажмите кнопку "Сохранить".

Для подключения к серверу доступа:

1. В главном окне приложения (см. стр. **15**) нажмите индикатор подключения.

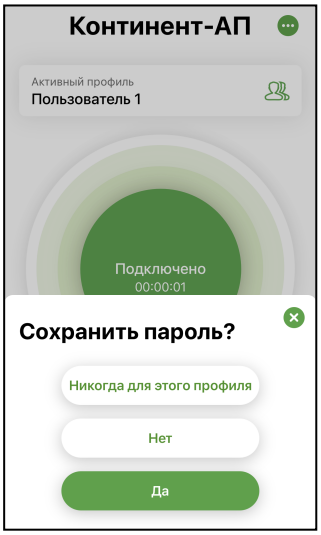
   На экране появится окно аутентификации. В зависимости от типа аутентификации, указанного в настройках профиля, приложение будет запрашивать логин и пароль или пароль для доступа к ключевому контейнеру.

   Примечание. В данном примере рассматривается вариант ввода логина и пароля.



2. Введите логин и пароль. Нажмите "Подключиться".

   Если в настройках профиля опция "Сохранить пароль" деактивирована, на экране появится окно, подобное следующему.



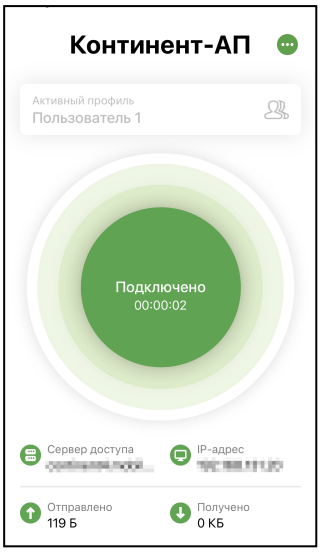
3. Выполните одно из следующих действий:
   - нажмите "Да".

     Пароль будет сохранен;
   - нажмите "Нет".

     Окно закроется, но при следующем подключении появится снова;
   - нажмите "Никогда для этого профиля".

     Уведомление закроется и больше появляться не будет.

Если логин и пароль введены правильно, главное окно "Континент-АП" примет вид, подобный следующему.

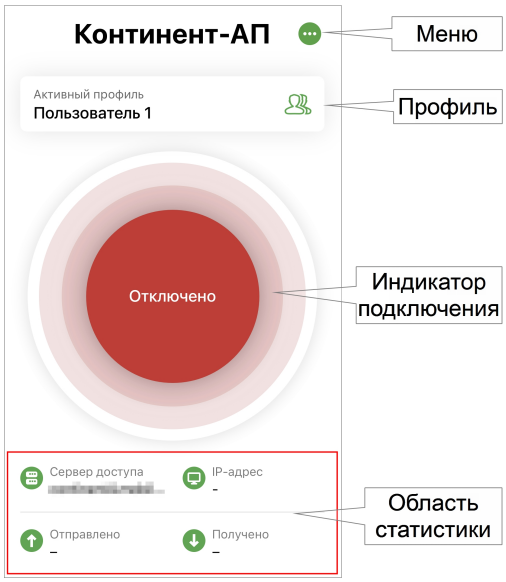


При активном подключении нельзя переходить в разделы "Сертификаты" и "Настройки".

Примечание. Раз в полгода пользователь должен менять пароль ключевого контейнера. При подключении к серверу доступа пользователь аутентифицируется и вводит пароль, происходит проверка и, если срок действия пароля истек, появляется окно, в котором пользователь должен ввести и подтвердить новый пароль.

Глава 3
Эксплуатация

Главное окно приложения



Описание главного окна

Главное окно состоит из четырех объектов:

Объект	Описание
Меню	Меню содержит разделы для работы с сертификатами, настройки подключения, просмотра журналов, сведений о программе и смены режима работы
Профиль	Просмотр, создание, удаление и настройка профилей подключения
Индикатор подключения	Подключение/отключение к/от СД
Область статистики	Просмотр статистики текущей сессии

Меню главного окна содержит следующие разделы:

Пункт меню	Описание
Сертификаты	Открывает окно с установленными сертификатами (см. стр. **19**). Раздел предназначен для удаления, запроса и импорта сертификатов и ключа, для сокрытия сертификатов и ключевых контейнеров в скрытой папке, просмотра информации о сертификате
Настройки	Открывает окно просмотра и настройки общих параметров подключения (см. стр. **25**)
Сменить режим работы	Включает и выключает режим ограниченного доступа к управлению настройкой "Континент-АП" — частный режим (см. стр. **31**). Основной режим устанавливается по умолчанию
Журнал	Открывает окно просмотра журнала (см. стр. **29**)
О программе	Выводит на экран сведения о текущей версии программного обеспечения и контрольные суммы динамических библиотек абонентского пункта

Окно "Профили"

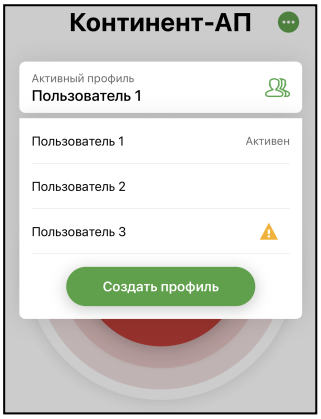
Список профилей

Примечание. "Континент-АП" поддерживает возможность создания профиля без привязки к сертификату. Такой профиль нельзя активировать, и в списке профилей он обозначается знаком ⚠.

Для перехода к списку профилей:

- В главном окне приложения выберите панель "Профиль".

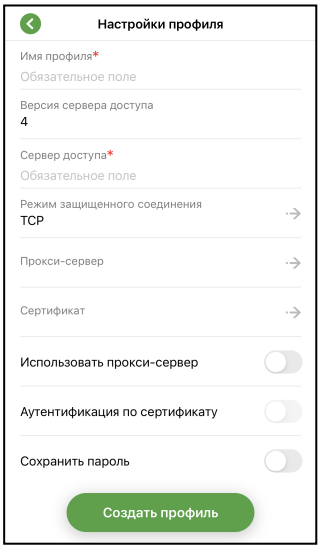
  На экране появится список профилей, подобный следующему.



Для создания профиля:

1. В списке профилей нажмите "Создать профиль".

   На экране появится окно, подобное следующему.



2. Активируйте поле "Сертификат".

   В появившемся окне появятся списки корневых и пользовательских сертификатов.

3. Выберите сертификат.

   В зависимости от выбранного типа сертификата версия СД заполняется автоматически и устанавливается переключатель "Аутентификация по сертификату". Если был выбран пользовательский сертификат для СД версии 3.x, версию СД можно изменить на 4.

Примечание. Настройки параметров профиля в зависимости от выбранного типа сертификата различаются следующим образом:

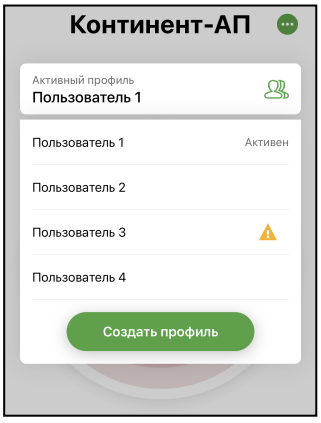
- если выбран пользовательский сертификат для СД 4.x, то активируется переключатель "Аутентификация по сертификату". Если деактивировать переключатель "Аутентификация по сертификату", аутентификация будет производиться по логину и паролю;
- если выбран пользовательский сертификат для СД 3.x, то переключатель "Аутентификация по сертификату" активируется и блокируется. Деактивировать его нельзя, доступна аутентификация только по сертификату;
- если выбран самоподписанный корневой сертификат для СД 4.x, то переключатель "Аутентификация по сертификату" деактивируется и блокируется. Активировать его нельзя, доступна аутентификация только по логину и паролю. Логин и пароль администратор передает пользователю по защищенному каналу.

4. Для настройки подключения через прокси-сервер:
   - для параметра "Режим защищенного соединения" укажите значение "TCP";

     Примечание.
     - Для СД 4.x значение "TCP" указано по умолчанию и не может быть изменено.
     - Для СД 3.x значение параметра можно изменить на "UDP".
     - При выборе значения "UDP" строка "Прокси-сервер" и переключатель "Использовать прокси-сервер" становятся скрытыми.

   - активируйте строку "Прокси-сервер";
   - в открывшейся группе параметров введите их значения;
   - нажмите кнопку "Сохранить";
   - в настройках профиля для параметра "Использовать прокси-сервер" укажите значение "ВКЛ".
5. Для ввода дополнительных параметров установите отметку в поле "Дополнительно" и введите их значение.
6. Заполните оставшиеся пустыми поля.
7. Нажмите кнопку "Создать профиль".

   Профиль появится в списке.

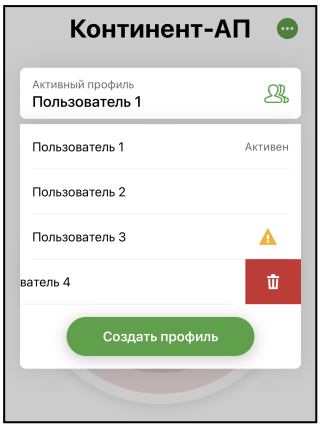


Для удаления профиля:

Примечание. Активный профиль удалить нельзя!

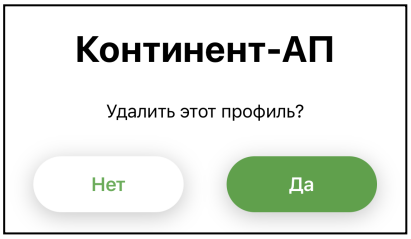
1. В списке профилей проведите пальцем справа налево по удаляемому профилю.

Окно примет вид, подобный следующему.



2. Нажмите  .

   На экране появится сообщение, подобное следующему.



3. Нажмите "Да".

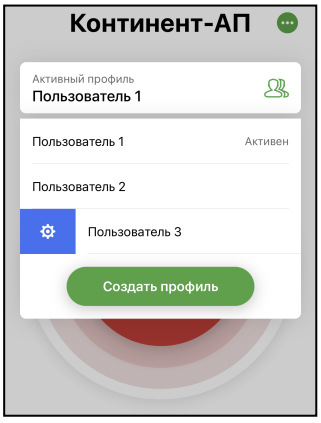
   Профиль будет удален.

Для настройки профиля:

Примечание. Редактирование профиля запрещено при установленном соединении с СД.

1. В списке профилей проведите пальцем слева направо по выбранному профилю.

   Окно примет вид, подобный следующему.



2. Нажмите  .

   На экране появится окно "Настройки профиля".

3. Внесите исправления в доступные для редактирования строки.
4. Нажмите "Сохранить".

Для смены активного профиля в приложении:

- В списке профилей нажатием выберите нужный профиль.
  Выбранный профиль отобразится на панели "Активный профиль".

Примечание. Активировать профиль без сертификата нельзя. Профиль без сертификата отмечается знаком .

Окно "Сертификаты"

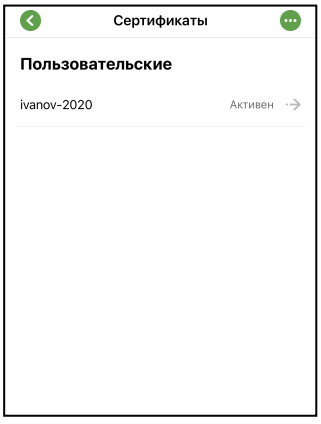
Описание окна

Окно содержит список всех импортированных на устройство пользовательских и корневых сертификатов. Актуальное состояние сертификатов отображается на экране рядом с названием сертификата. Для отображения состояния используются следующие отметки:

Отметка	Значение
Активен	Статус присваивается, если пользовательский сертификат актуален и используется устройством в данный момент
Срок действия истекает через n дней	Предупреждение появляется за 14 дней до окончания срока действия сертификата, n — переменная, обозначающая количество дней
Отозван по CRL	Сертификат находится в списке недействительных сертификатов
Просрочен	Срок действия сертификата истек
Нет CRL	Данный сертификат не прошел проверку по CRL
CRL просрочен	Срок действия CRL истек или еще не начался
Не активен	Срок действия сертификата еще не начался

Для работы с сертификатами:

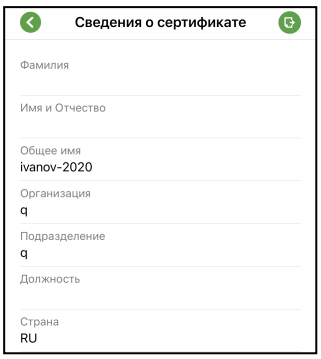
- В главном окне приложения откройте меню и выберите "Сертификаты".
  Откроется окно "Сертификаты".



Для просмотра сведений о пользовательском сертификате:

- Выберите его в списке.

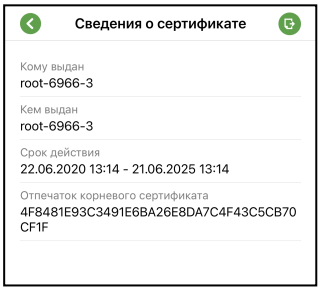
  Окно примет вид, подобный следующему.



Для просмотра сведений о корневом сертификате:

- Выберите его в списке.

  Окно примет вид, подобный следующему.



Примечание. Корневые сертификаты бывают двух видов:
- из полного набора, связанные с пользовательским сертификатом;
- самоподписанные.

В окне "Сертификаты" отображаются пользовательские и самоподписанные корневые сертификаты. Для просмотра информации о корневом сертификате, который связан с пользовательским, в окне "Сведения о сертификате" нажмите "Корневой сертификат".

Для удаления сертификата:

1. В окне "Сертификаты" проведите пальцем справа налево по строке удаляемого сертификата.
2. Нажмите  .
3. Нажмите "ОК".

   Сертификат будет удален.

Для экспорта сертификата:

Примечание. Операция "Экспорт сертификата" предназначена для передачи сертификата в техническую поддержку в случае ошибки подключения пользователя к серверу доступа.

1. Перейдите в окно сведений о сертификате.
2. Нажмите  .

   "Континент-АП" предложит выбрать приложение для отправки сертификата.
3. Откроется стандартный почтовый клиент.

   Автоматически будут заполнены строки "От", "Тема" и вложен файл сертификата.
4. Введите адрес получателя и отправьте письмо.

Скрытие сертификатов

Процедура предназначена для защиты файлов от несанкционированного изменения, удаления или передачи. После выполнения процедуры при открытии папки приложения файлы user.cer, root.p7b и user.key будут невидимы для пользователя, в том числе и при подключении к компьютеру. Чтобы отменить процедуру скрытия файлов, повторите ее еще раз.

Примечание. При удалении "Континент- АП" все файлы приложения, включая скрытые сертификаты, будут удалены.

Для скрытия файлов:

1. Откройте окно "Сертификаты".
2. Проведите пальцем слева направо по строке требуемого сертификата.

3. Нажмите  .

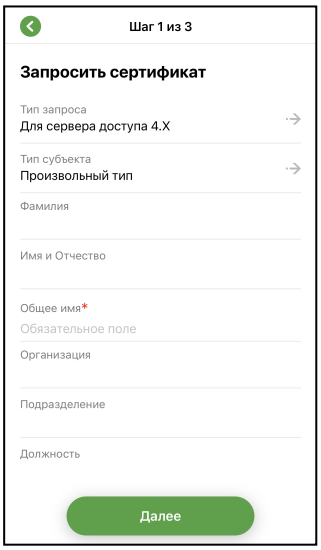
   Рядом со скрытыми сертификатами появится значок  .

Меню окна "Сертификаты"

Запрос на сертификат

Для создания запроса на сертификат:

1. В меню окна "Сертификаты" нажмите "Создать запрос на сертификат".



   В зависимости от выбранного типа субъекта внешний вид страницы запроса будет различаться.

2. Введите сведения о пользователе.

   Для ввода сведений активируйте поле нажатием и используйте экранную клавиатуру.

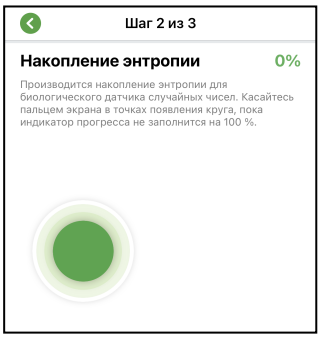
Примечание. Тип запроса зависит от версии СД.

В зависимости от выбранного типа субъекта обязательными являются следующие поля:

Атрибут	Произвольный тип	ФЛ	ФЛ (ЮЛ)	ИП	ЮЛ
Тип запроса	+	+	+	+	+
Фамилия		+	+	+	
Имя и Отчество		+	+	+	
Общее имя	+		+		+
Организация		+			
Подразделение					
Должность			+		
Страна	+	+	+	+	+
Область			+		+
Населенный пункт			+		+
Адрес			+		+
Электронная почта					
ИНН			+		+
СНИЛС		+		+	
ОГРН			+		+
ОГРНИП				+	

3. Нажмите "Далее".

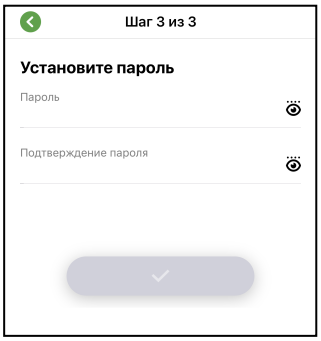
   На экране появится окно, подобное следующему.



4. Нажимайте на мишень, пока индикатор прогресса не заполнится целиком.

   Примечание. Непопадание в круг может привести к снижению уровня накопленной энтропии и повторному выполнению операции.

   Когда индикатор покажет 100%, откроется диалог задания пароля для доступа к ключевому контейнеру.



5. Введите и подтвердите пароль.

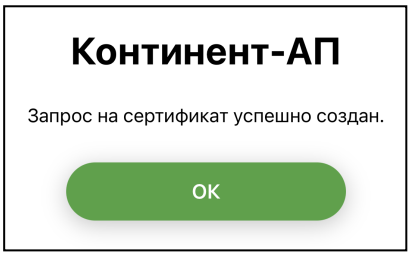
Примечание. Минимальные требования к паролю:
- длина пароля должна быть не менее 6 символов;
- пароль должен содержать буквы латинского алфавита (A–Z, a–z), арабские цифры (0–9) и следующие символы: **? ! : ; " ' , . < > / { } [ ] ~ @ # $ % ^ & * - _ + = \ ` | № ( )**;
- буквенная часть пароля должна содержать как строчные, так и прописные буквы.

6. Нажмите .

   В нижней части экрана появится меню, подобное следующему.

7. Нажмите "Отправить".

   На экране появится сообщение, подобное следующему.



8. Нажмите "ОК".

   Откроется стандартный почтовый клиент.

9. В окне почтового клиента впишите адрес и отправьте письмо администратору. Автоматически будут заполнены строки "От", "Тема" и вложен файл запроса на сертификат.

Примечание. Администратор передает один из наборов файлов:
- полный набор — пользовательский и корневой сертификаты;
- самоподписанный корневой сертификат.

Импорт сертификата

Для импорта сертификата:

Примечание. При импорте архива с сертификатами из почты убедитесь, что внутри архива нет других папок.

1. Откройте меню окна "Сертификаты" и выберите пункт "Импортировать сертификат".

   На экране появится содержимое папки приложения "Континент-АП".

2. Выберите нужную папку и нажмите "Выбрать".

   На экране появится окно "Сертификаты". В списке сертификатов появятся новые пользовательские и корневые сертификаты. Количество и тип сертификатов зависит от набора, переданного администратором.

Импорт ключа

Операция предназначена для случая, когда администратор сформировывает файлы, включая ключ, без запроса на сертификат. Тогда для корректной работы приложения пользователь должен конвертировать ключ в формат для мобильного "Континент-АП". Если ключ не конвертировать, то подключение к СД осуществляться не будет.

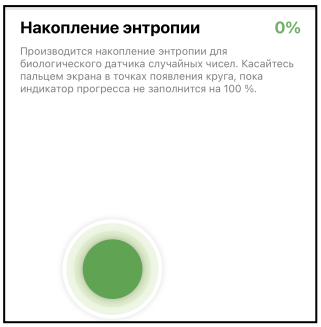
Для импорта ключа:

1. В меню окна "Сертификаты" выберите пункт "Импортировать ключ".

   На экране появится содержимое папки приложения "Континент-АП".

2. Выберите папку и нажмите "Выбрать".

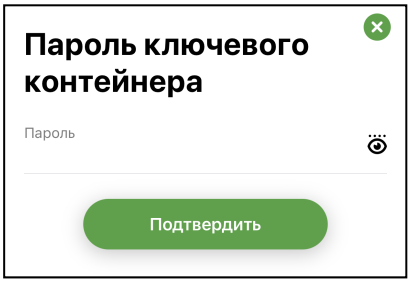
На экране появится окно, подобное следующему.



3. Нажимайте на мишень, пока индикатор прогресса не заполнится целиком.

Пояснение. Непопадание в круг может привести к снижению уровня накопленной энтропии и повторному выполнению операции.

Когда индикатор покажет 100%, откроется запрос на ввод пароля для доступа к ключевому контейнеру.



4. Введите пароль, полученный от администратора, и нажмите "Подтвердить".

   Операция будет завершена и появится сообщение об успешном импорте.

5. Нажмите "ОК".

   В папке сохранится ключ в формате user.key.

Импорт CRL

Импорт CRL выполняется пользователем вручную с использованием файла со списком отозванных сертификатов, полученным от администратора.

Примечание. Перед выполнением процедуры импорта CRL необходимо включить параметр "Проверка по CRL" (см. стр. 10) в разделе "Настройки подключения".

Для импорта файла CRL:

1. В меню окна "Сертификаты" нажмите "Импортировать CRL".

   На экране появится содержимое папки приложения "Континент-АП".

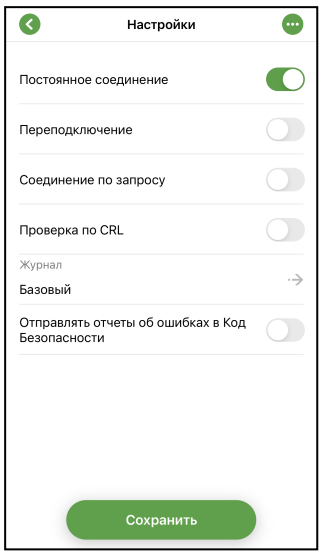
2. Выберите нужную папку и нажмите "Выбрать".

   После успешного завершения операции на экране появится соответствующее сообщение.

3. Нажмите "ОК".

Окно "Настройки"

В окне выполняется настройка параметров подключения к серверу доступа и настройка детализации журналирования. Операции импорта конфигурации, экспорта и импорта настроек выполняются из меню.



Импорт конфигурации

Файл конфигурации собирается на СД в зашифрованном или незашифрованном виде, в зависимости от версии СД, и содержит следующие компоненты:

Компонент	Параметры
Версия конфигурации	Номер версии
Профили	**1.** Название. **2.** Признак профиля по умолчанию. **3.** Признак глобального профиля. **4.** Логин. **5.** Идентификатор (UUID) пользовательского сертификата. **6.** Адреса серверов доступа: • название; • имя хоста; • порт TCP; • порт UDP
Ключевые контейнеры	**1.** Идентификатор (UUID). **2.** Ключевой контейнер. **3.** Имя ключевого контейнера. **4.** Случайное число для формирования ключевого контейнера
Сертификаты	**1.** Пользовательские. **2.** Серверные. **3.** Промежуточные корневые. **4.** Корневые

Файл конфигурации для быстрого старта содержит профили, ключевой контейнер и сертификаты.

Сервер доступа версия 3	Сервер доступа версия 4
Всегда зашифрован	Шифрование опционально
На устройстве всегда набирается энтропия	Энтропия набирается на сервере при формировании файла
Расширение XXX.apcfg	Расширение XXX.ts4

Ниже рассмотрен общий порядок действий при импорте файла конфигурации.

Импорт конфигурации для быстрого старта

Для импорта конфигурации:

1. Администратор формирует файл конфигурации и передает пользователю по почте или на съемном носителе. Если конфигурация зашифрована, администратор сообщает пользователю пароль от конфигурации и пароли ключевых контейнеров по доверенному каналу.
2. Пользователь переносит полученный файл конфигурации на устройство.
3. Пользователь запускает приложение "Континент-АП" и нажимает кнопку "Импортировать файл" на экране загрузки. Пользователь находит файл конфигурации в папке приложения "Континент-АП", выбирает его и нажимает кнопку "Выбрать".
4. Приложение определяет тип конфигурации. Если файл сформирован на СД версии 3, на устройстве появится окно с накоплением энтропии. Если файл сформирован на СД версии 4, шаг с накоплением энтропии пропускается.
5. На этом этапе при необходимости пользователь вводит пароль от конфигурации.
6. Пользователь вводит пароль от ключевого контейнера, так как ключ импортируется из конфигурации и конвертируется в формат для "Континент-АП".
7. Приложение "Континент-АП" извлекает сертификаты и ключевой контейнер в скрытую папку. В интерфейсе новые сертификаты импортируются в раздел "Сертификаты", создается новый профиль.

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит соответствующее сообщение.

Если импорт конфигурации для быстрого старта выполняется повторно:

- старые сертификаты, ключевые контейнеры на устройстве и ссылки на сертификаты в приложении не удаляются;
- профиль из конфигурации добавится с именем <имя_профиля>+1, а старый профиль останется.

Восстановление настроек

Если в результате действий пользователя или администратора были нарушены настройки профиля или удалены сертификаты, выполните повторный импорт конфигурации. Настройки профиля и сертификаты на устройстве будут восстановлены.

Экспорт настроек

Внимание! Данная функция предназначена для переноса настроек с одного устройства на другое исключительно для одного конкретного пользователя. Нельзя передавать файл с настройками другим пользователям.

Экспорт настроек предназначен для переноса готового набора профилей, сертификатов и ключевых контейнеров на новое устройство. Операция "Экспортировать настройки" предшествует операции "Импортировать настройки". В отличие от файла конфигурации файл настроек формируется на устройстве и имеет формат "settings.csf".

Для экспорта настроек:

1. Вызовите меню окна "Настройки".
2. Нажмите "Экспортировать настройки".

   Приложение предложит выбрать папку для сохранения файла.
3. Отметьте папку и нажмите "Выбрать".

На экране появится сообщение об успешном сохранении файла. Приложение вернет пользователя в окно "Настройки подключения".

Сохраненный файл извлеките из памяти устройства любым доступным способом и передайте на другое устройство для выполнения операции импорта.

Импорт настроек

Внимание! Данная функция предназначена для переноса настроек с одного устройства на другое исключительно для одного конкретного пользователя. Нельзя передавать файл с настройками другим пользователям.

Операция предназначена для установки пакета настроек из другого приложения. Перед выполнением импорта создайте папку и разместите в ней файл настроек "settings.csf".

Для импорта настроек:

1. Вызовите меню окна "Настройки".
2. Нажмите "Импортировать настройки".

   Внимание! Импорт настроек заменит все текущие настройки на настройки из импортируемого файла.

   Откроется содержимое папки приложения "Континент-АП".
3. Выберите в папке файл настроек и нажмите кнопку "Выбрать".

   Примечание. После импорта настроек все сертификаты импортируются скрытыми (см. стр. 21).

Глава 4
Служебные операции

Обновление

Обновление приложения "Континент-АП" выполняется при переходе на новую версию в стандартном магазине приложений "App Store".

Примечание.

- В зависимости от настроек устройства пользователя, приложения могут обновляться автоматически. Проверить версию "Континент-АП", установленную на устройстве, можно в разделе приложения "О программе".
- Для работы с App Store необходимо наличие Apple ID.

Для обновления приложения вручную:

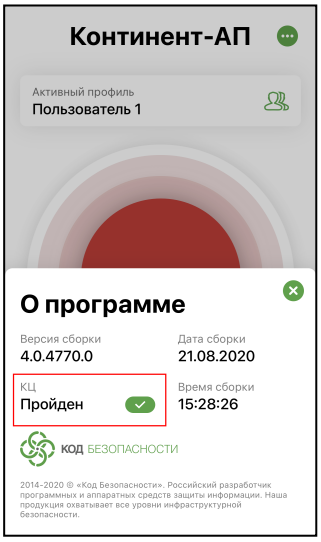
- В магазине приложений "App Store " найдите приложение "Континент-АП" и выполните стандартную процедуру обновления.

Контроль целостности

Контроль целостности (далее — КЦ) файлов заключается в сравнении текущих значений контрольных сумм с эталонными значениями контрольных сумм динамических библиотек, заранее вычисленных при установке приложения на устройстве.

Для проведения КЦ приложения:

1. В главном окне откройте меню (см. стр. **15**) и выберите пункт "О программе".
2. В появившемся окне нажмите на область, указанную на рисунке ниже.



Откроется окно "Список файлов".

3. Нажмите кнопку "Проверить целостность".

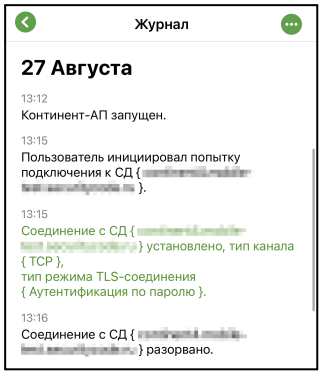
При обнаружении нарушения КЦ работа приложения блокируется, в журнале записывается соответствующее событие. Для восстановления работы необходимо переустановить приложение.

Если КЦ пройден успешно, появится соответствующее сообщение.

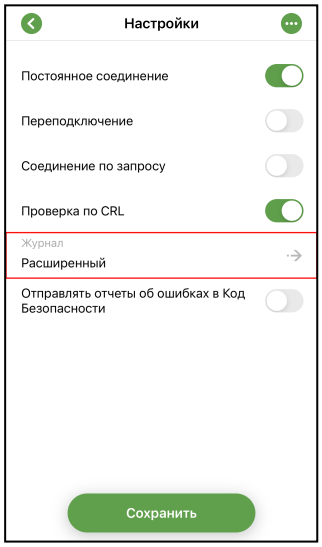
Журнал

Журнал работы приложения

В окне "Журнал" содержатся сведения о работе приложения "Континент-АП" за период работы с момента установки приложения.



В журнале предусмотрены два уровня детализации: базовый и расширенный.



Расширенный уровень детализации включается в разделе "Настройки подключения" (см. стр. **10**). Все возможные события, уровень их детализации и цветовое обозначение представлены в таблице ниже.

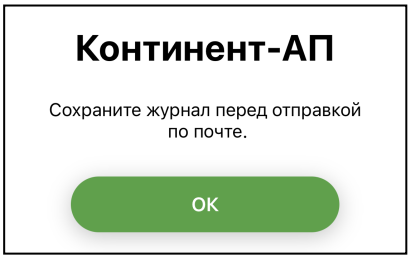
Уровень детализации	Цвет	Событие
Базовый	Черный	"Континент-АП" запущен
Базовый	Черный	Добавлена ссылка на папку с сертификатом пользователя
Базовый	Черный	Удалена ссылка на папку с сертификатом пользователя
Базовый	Черный	Соединение с СД разорвано
Базовый	Черный	Пользователь инициировал попытку подключения к СД
Базовый	Черный	Добавлена ссылка на папку с корневым сертификатом
Базовый	Черный	Удалена ссылка на папку с корневым сертификатом
Базовый	Зеленый	Соединение с СД установлено

Уровень детализации	Цвет	Событие
Базовый	Зеленый	Пользователь создал запрос на сертификат и ключевой контейнер
Базовый	Красный	Произошла системная ошибка
Базовый	Красный	Ошибка аутентификации пользователя
Расширенный	Черный	Пользователь внес изменения в настройки проверки сертификатов
Расширенный	Черный	Пользователь импортировал CRL из файла
Расширенный	Черный	Проверка целостности файла выполнена успешно
Расширенный	Черный	Выполнен перерасчет контрольной суммы файла
Расширенный	Черный	Пользователь изменил параметры подключения к СД
Расширенный	Зеленый	Запуск процедуры проверки целостности файлов выполнен успешно
Расширенный	Красный	СД не ответил на отклик за указанное время
Расширенный	Красный	СД разорвал соединение с АП
Расширенный	Красный	Ошибка подключения: использован неподдерживаемый на СД режим организации VPN-соединения
Расширенный	Красный	Нарушена целостность файла. Создание новых сессий запрещено

Для отправки журнала в техническую поддержку:

1. В окне "Журнал" откройте меню и нажмите "Отправить журнал".

   Откроется окно, подобное следующему.



2. Нажмите "ОК".

   Откроется содержимое папки приложения "Континент-АП".

3. Выберите папку или создайте новую. Нажмите "Выбрать".

   Файл журнала "continentra-journal.log" будет создан и сохранен в указанную папку. Откроется стандартный почтовый клиент. Автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.

4. В окне почтового клиента впишите адрес и отправьте письмо администратору.

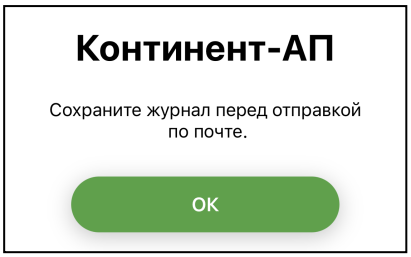
Отладочный журнал

Отладочный журнал предназначен для проведения детального анализа в случае сбоя в работе приложения.

Для отправки журнала в техническую поддержку:

1. В окне "Журнал" откройте меню и нажмите "Отправить отладочный журнал".

Откроется окно, подобное следующему.



2. Нажмите "ОК".

   Откроется содержимое папки приложения "Континент-АП".

3. Выберите папку или создайте новую. Нажмите "Выбрать".

   Файл журнала "continentra-debug-journal.log" будет создан и сохранен в указанную папку. Откроется стандартный почтовый клиент. Автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.

4. В окне почтового клиента впишите адрес и отправьте письмо администратору.

Управление режимом работы

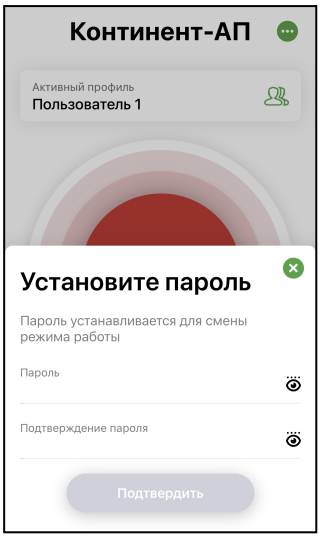
"Континент-АП" функционирует в двух режимах:

Основной режим
Устанавливается по умолчанию.Пользователю предоставляются права полного доступа. Права в основном режиме: • подключение и отключение от СД; • просмотр списка профилей; • активация профиля; • просмотр информации о профиле и редактирование; • удаление профиля; • экспорт/импорт настроек; • импорт конфигурации; • создание запроса на сертификат; • импорт сертификата; • просмотр импортированных сертификатов; • просмотр сведений о сертификате; • импорт ключа; • импорт CRL; • удаление сертификата; • скрытие сертификата в скрытой папке; • просмотр и редактирование настроек подключения; • смена режима работы; • просмотр и сохранение журнала; • просмотр раздела "О программе"
Режим ограниченной функциональности
Пользователю предоставляются права ограниченного доступа к управлению настройками приложения. Права в режиме ограниченной функциональности: • подключение и отключение к/от СД по заранее активированному профилю; • просмотр и сохранение журнала; • просмотр раздела "О программе"

Для смены режима работы:

1. Откройте меню приложения "Континент-АП".
2. В появившемся меню выберите пункт "Сменить режим работы".

На экране появится окно "Установите пароль".



3. Введите пароль блокировки в поля "Пароль" и "Подтверждение пароля".
4. Нажмите "Подтвердить".

   На главном экране появится надпись "Режим ограниченной функциональности" на синем фоне, функции приложения будут ограничены.

Для смены режима работы повторите предыдущую операцию еще раз. Если надпись "Режим ограниченной функциональности" не отображается в главном окне приложения, активирован основной режим.