КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

Континент-АП

Версия 4 (исполнение 7)

Руководство администратора

Аврора

RU.АМБС.58.29.12.005 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

Введение

Документ предназначен для администраторов изделия "Средство криптографической защиты информации "Континент-АП". Версия 4 (исполнение 7)" RU.АМБС.58.29.12.005. В нем содержатся сведения, необходимые для установки, настройки и эксплуатации абонентского пункта на платформе ОС Аврора 3.x.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-800-505-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании — https://www.securitycode.ru/services/tech-support/.

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

Средство криптографической защиты информации "Континент-АП" (далее — "Континент-АП", приложение) входит в состав изделия "Аппаратно-программный комплекс шифрования "Континент"(далее — АПКШ "Континент") и обеспечивает доступ удаленных пользователей, использующих мобильные устройства, к информационным ресурсам корпоративной сети, защищенной средствами АПКШ "Континент".

Для организации доступа удаленных пользователей к ресурсам защищаемой сети используется сервер доступа, входящий в состав АПКШ "Континент".

Программное обеспечение абонентского пункта реализовано в виде приложения "Континент-АП". Приложение устанавливается на мобильные устройства, функционирующие под управлением операционной системы (ОС) Аврора 3.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 — в соответствии с ГОСТ 28147-89, длина ключа — 256 бит;
- защита передаваемых данных от искажения — в соответствии с 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.

Профили

Перед установлением соединения с сервером доступа выполните настройку параметров подключения.

Назначение параметров подключения разъясняется в таблице ниже:

Параметр	Описание	
Имя профиля	Название профиля для подключения к серверу доступа	
Версия сервера доступа	Номер версии сервера доступа, к которому будет подключаться пользователь. Версия сервера заполняется автоматически	
Сервер доступа	IP-адрес или имя сервера доступа	
Режим защищенного соединения	Способ подключения абонентского пункта к серверу доступа: • стандартное подключение (UDP); • потоковое подключение (TCP); • подключение через прокси (только для TCP)	
Прокси-сервер	Признак использования прокси-сервера для подключения к серверу доступа. Хранит имя или IP-адрес прокси-сервера. Доступен только при режиме защищенного соединения через TCP. При нажатии на строку параметра открывается окно настроек подключения к прокси-серверу:	
	Адрес	Сетевое имя или IP-адрес прокси-сервера
	Порт	Порт прокси-сервера. По умолчанию устанавливается значение 3128
	Аутентификация	Тип аутентификации: • без аутентификации; • Basic; • NTML
	Имя пользователя	Имя пользователя для аутентификации на прокси-сервере
	Пароль	Пароль пользователя для аутентификации на прокси-сервере
Сертификат	Необходимый для подключения к серверу доступа сертификат пользователя. Список доступных сертификатов представляет собой список импортированных сертификатов	
Аутентификация по сертификату	Параметр отвечает за аутентификацию по паролю от ключевого контейнера	
Сохранить пароль	Сохраняет пароль от подключения к серверу доступа	
Дополнительные настройки	При активации делает доступными следующие настройки: порт сервера доступа, порт клиента, основной DNS-сервер, альтернативный DNS-сервер, домен, MTU	
Порт сервера доступа	Порт сервера доступа. По умолчанию устанавливаются значения 443 для TCP и 4433 для UDP	
Порт клиента	Порт мобильного устройства. По умолчанию устанавливается значение 7500	

Параметр	Описание
Основной DNS-сервер, альтернативный DNS-сервер	По умолчанию используются адреса DNS-серверов, получаемые от сервера доступа. Если адреса от сервера доступа не поступают, их указывают вручную. Адреса, полученные от сервера доступа, имеют приоритет над адресами, указанными вручную
Домен	DNS-суффикс. По умолчанию не используется. При необходимости можно указать DNS-суффикс, добавляемый автоматически к имени хоста при обращении к защищаемым ресурсам
MTU	Максимальный размер блока (в байтах) на канальном уровне сети. По умолчанию устанавливается значение 1500

Так как параметры подключения изменяются (например, подключение к разным серверам доступа, использование разных сертификатов и т. д.), для каждого подключения предварительно устанавливаются конкретные значения параметров и сохраняются в виде профиля настроек с присвоенным ему именем.

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

Для использования нового профиля при подключении к серверу доступа присвойте ему статус "Активен". Статус "Активен" может быть назначен только профилю с привязанным сертификатом. При подключении профиль со статусом "Активен" используется по умолчанию.

Настройки подключения

Перед установлением соединения с сервером доступа выполняется настройка общих параметров, действующих для всех подключений.

Назначение настроек подключения разъясняется в таблице ниже:

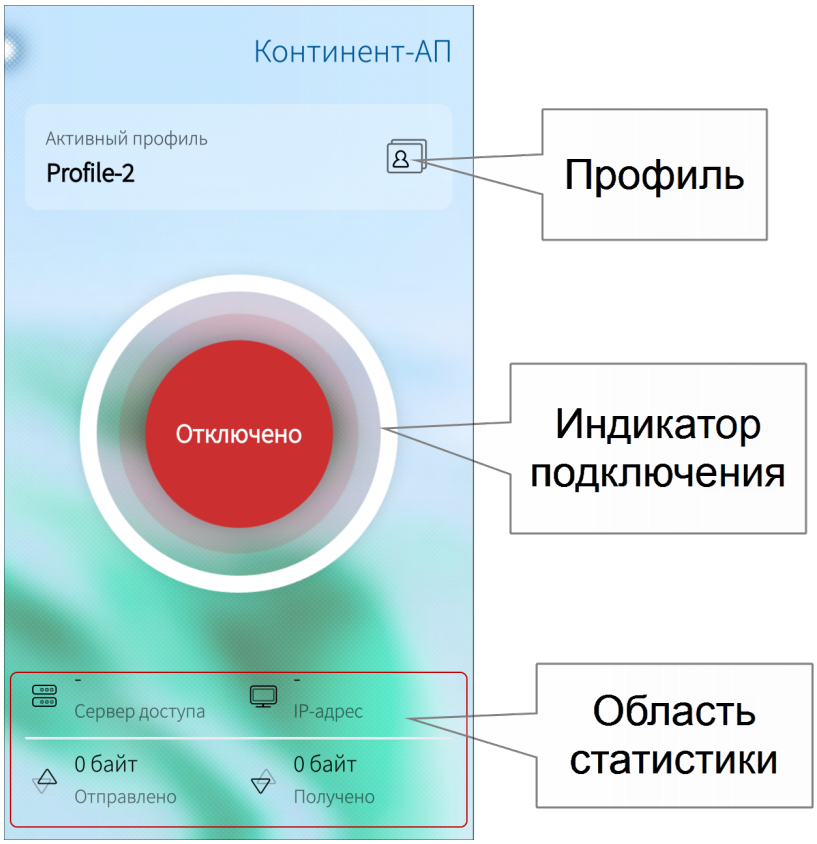
Параметр	Описание
Постоянное соединение	Соединение отключается только средствами настройки общих параметров подключения и автоматически восстанавливается после потери сетевого соединения. Для реализации постоянного соединения с сервером доступа предварительно настройте или активируйте профиль подключения. Параметр имеет одно из двух значений: "Да" (есть отметка) или "Нет" (отметка отсутствует). Применение параметра блокирует управление некоторыми другими параметрами подключения
Переподключение	Автоматическое переподключение при потере сетевого соединения или при разрыве защищенного канала по инициативе сервера доступа АПКШ "Континент". Параметр может принимать два значения: "Да" (есть отметка) или "Нет" (отметка отсутствует). Недоступно для управления, если установлен параметр "Постоянное соединение"
Количество попыток переподключения	По умолчанию равно 3 (трем). При необходимости может быть изменено. После последней неудачной попытки выводится сообщение об ошибке подключения. Недоступно для управления, если установлен параметр "Постоянное соединение"
Тайм-аут переподключения	Пауза между попытками подключения (в секундах). По умолчанию устанавливается значение 30. Недоступно для управления, если установлен параметр "Постоянное соединение"

Параметр	Описание
Тайм-аут неактивности	Время неактивности (в секундах), по истечении которого произойдет отключение от сервера доступа (под неактивностью понимается отсутствие трафика в защищенном канале). По умолчанию установлено значение 600. Недоступно для управления, если установлен параметр "Постоянное соединение"
Проверка по CRL	Параметр принимает значение вкл/выкл. Предназначен для проверки актуальности сертификата по списку отозванных сертификатов
Журнал	Параметр предназначен для увеличения детализации аудита и принимает значения базовый/расширенный

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 АПКШ "Континент". Операция импорта применяется для загрузки на конкретное устройство настроек приложения, экспортированных с другого устройства с установленным "Континент-АП".

Глава 2
Эксплуатация

Главное окно приложения



Описание главного окна приложения

Центральная часть окна состоит из четырех объектов:

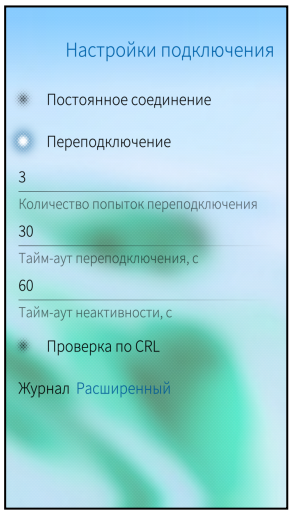
Объект	Описание
Меню	Меню содержит разделы для работы с сертификатами, настройки подключения, проведения обновления, просмотра журналов, сведений о программе и смены режима работы
Профиль	Просмотр, создание, удаление и настройка профилей подключения
Индикатор подключения	Подключение и отключение от сервера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

Ниже в таблице приводится полный список пунктов меню:

Пункт меню	Описание
Главная	Открывает главное окно приложения
Сменить режим работы	Включает и выключает режим ограниченного доступа к управлению настройкой "Континент-АП" — частный режим (см. стр.31). Основной режим устанавливается по умолчанию

Пункт меню	Описание
Профили	Открывает окно с профилями (см. стр.**15**), в котором можно просматривать, создавать, удалять и настраивать профили подключения
Сертификаты	Открывает окно с установленными сертификатами (см. стр.**19**). Раздел предназначен для удаления, запроса и импорта сертификатов, ключа и CRL, просмотра информации о сертификате
Настройки подключения	Открывает окно просмотра и настройки общих параметров подключения (см. стр.**10**)
Экспорт настроек	Переносит готовый набор профилей, сертификатов и ключевых контейнеров на новое устройство
Импорт настроек	Устанавливает пакет настроек из другого приложения
Импорт конфигурации	Предназначен для быстрого старта, обновления сертификатов и профилей
Журнал	Открывает окно просмотра журнала (см. стр.**28**)
Обновление ПО	Запускает процедуру обновления программного обеспечения "Континент-АП" (см. стр.**25**)
О программе	Выводит на экран сведения о текущей версии программного обеспечения и контрольные суммы динамических библиотек абонентского пункта (см. стр.**26**)

Окно "Настройки подключения"



В окне выполняется настройка параметров подключения к серверу доступа и настройка детализации журналирования.

Импорт конфигурации

Файл конфигурации собирается на сервере доступа. В зависимости от версии сервера доступа файл формируется в зашифрованном или незашифрованном виде.

Файл конфигурации 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

Комбинации компонентов файла конфигурации зависят от поставленных задач:

- для быстрого старта файл конфигурации включает профили, ключевой контейнер и сертификаты;
- для обновления сертификатов файл конфигурации включает сертификаты и ключевые контейнеры;
- для обновления настроек профиля файл конфигурации включает профили. Для получения ключевого контейнера и сертификатов пользователь оформляет запрос;
- для ответа на запрос пользователя файл конфигурации включает профили и сертификаты, ключевой контейнер создается на устройстве пользователя.

Свойства файла конфигурации зависят от сервера доступа, на котором он был сформирован:

Сервер доступа версия 3	Сервер доступа версия 4
Всегда зашифрован	Шифрование опционально
На устройстве всегда набирается энтропия	Энтропия набирается на сервере при формировании файла
При формировании файла доступна комбинация компонентов для быстрого старта	Для формирования файла доступны все перечисленные комбинации
Расширение XXX.apcfg	Расширение XXX.ts4

Ниже рассмотрен общий порядок действий при импорте каждой комбинации 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 "Импорт файла" на экране загрузки.
4. Приложение определяет тип конфигурации. Если файл сформирован на сервере доступа версии 3, на устройстве появится окно с накоплением энтропии. Если файл сформирован на сервере доступа версии 4, шаг с накоплением энтропии пропускается.
5. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". 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".

   Примечание. В состав файла конфигурации может входить несколько ключевых контейнеров. Пользователь должен ввести пароль для каждого ключевого контейнера в наборе.
7. Приложение "Континент-АП" создает на устройстве скрытую папку с именем <имя пользователя_keyfingerprint> и извлекает в папку сертификаты и ключевой контейнер. В интерфейсе новые сертификаты импортируются в раздел "Сертификаты", создаются новые профили и статус "Активен"присваивается профилю с признаком по умолчанию.

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения с новым активным профилем.

Если импорт конфигурации для быстрого старта выполняется повторно:

- настройки существующего профиля заменятся новыми настройками из файла конфигурации;
- в настройках профиля изменится привязка к сертификатам. Требуется привязать профиль к новым сертификатам в соответствии с его настройками в файле конфигурации;
- старые сертификаты, ключевые контейнеры на устройстве и ссылки на сертификаты в приложении не удаляются.

Импорт конфигурации для обновления сертификатов

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 "Импорт конфигурации" в меню главного экрана приложения.
4. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". На этом этапе при необходимости пользователь вводит пароль от конфигурации.
5. Пользователь вводит пароль от ключевого контейнера, так как ключ импортируется из конфигурации и конвертируется в формат для "Континент-АП".

   Примечание. В состав файла конфигурации может входить несколько ключевых контейнеров. Пользователь должен ввести пароль для каждого ключевого контейнера в наборе.
6. Приложение "Континент-АП" создает на устройстве скрытую папку с именем <имя пользователя_keyfingerprint> и извлекает в папку сертификаты и ключевой контейнер. В интерфейсе сертификаты импортируются в раздел "Сертификаты".

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения.

При совпадении имен существующего и импортируемого сертификата:

- старые сертификаты, ключевые контейнеры на устройстве и ссылки на сертификаты не удаляются;
- привязка к сертификату в настройках профиля не изменяется.

Если пользователь произведет импорт такой конфигурации из экрана загрузки, для полной настройки приложения необходимо создать профиль. Окно создания профиля отобразится после импорта конфигурации.

Импорт конфигурации для обновления профиля

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 по доверенному каналу.
2. Пользователь переносит полученный файл конфигурации на устройство.
3. Пользователь запускает приложение "Континент-АП" и нажимает кнопку "Импорт конфигурации" в меню главного экрана приложения.
4. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". На этом этапе при необходимости пользователь вводит пароль от конфигурации.
5. Приложение "Континент-АП" извлекает из файла конфигурации информацию о настройках профиля и создает новые профили. Профили импортируются без привязки к сертификату и отмечаются знаком ⚠. При попытке активации профиля появится предупреждение: "Не указан сертификат для подключения".
6. Пользователь делает запрос на сертификат и импортирует полученные сертификаты в разделе "Сертификаты".
7. Пользователь редактирует импортированный профиль, привязывает сертификат к новому профилю и нажимает кнопку "Сохранить".

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения с новым активным профилем.

Если пользователь произведет импорт конфигурации с помощью экрана загрузки:

- приложение выдаст ошибку "В конфигурации не указан сертификат для подключения. Запросите и импортируйте сертификат".

Импорт конфигурации после запроса пользователя

Для импорта конфигурации:

1. Пользователь создает запрос на сертификат с помощью экрана загрузки и отправляет администратору.
2. Администратор на основе запроса формирует файл конфигурации и передает пользователю по почте или на съемном носителе. Если конфигурация зашифрована, администратор сообщает пользователю пароль от конфигурации по доверенному каналу.
3. Пользователь переносит полученный файл конфигурации на устройство.
4. Пользователь запускает приложение "Континент-АП" и нажимает кнопку "Импорт файла" на экране загрузки.
5. Пользователь находит файл конфигурации в памяти устройства, выбирает его и нажимает кнопку "Выбрать". На этом этапе при необходимости пользователь вводит пароль от конфигурации.

   Примечание. Если в папке отсутствует запрос на сертификат и ключевой контейнер, появится сообщение об ошибке "Не удается импортировать конфигурацию. Не найден ключевой контейнер".

   Приложение "Континент-АП" извлекает из файла конфигурации информацию о сертификате и настройках профиля. Файлы сертификатов

добавляются в папку с именем <имя пользователя>, которая была сформирована при запросе на сертификат.

6. В интерфейсе новые сертификаты импортируются в раздел "Сертификаты". В приложении создается новый профиль. Сертификат, соответствующий запросу, и ключевой контейнер привязываются к профилю автоматически. После установки настроек профиль принимает статус "Активен".

Если операция импорта выполнена успешно, приложение "Континент-АП" отобразит главный экран приложения с новым активным профилем.

Пользователь также может импортировать такую конфигурацию из экрана "Настройки подключения". Предварительно необходимо создать и отправить администратору запрос на сертификат.

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.

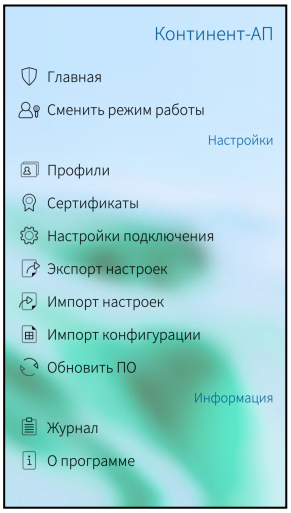
Экспорт настроек

Примечание. 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 "Экспорт настроек" предшествует операции "Импорт настроек". В отличие от файла конфигурации файл настроек формируется на устройстве и имеет формат continentra-settings.csf.

Для экспорта настроек:

1. Перейдите в меню главного окна приложения.



2. В появившемся окне нажмите "Экспорт настроек".

   Приложение предложит выбрать папку для сохранения файла.

3. Отметьте папку и нажмите "Выбрать".

   На экране появится сообщение об успешном сохранении файла. Приложение вернет пользователя на страницу главного окна приложения.

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

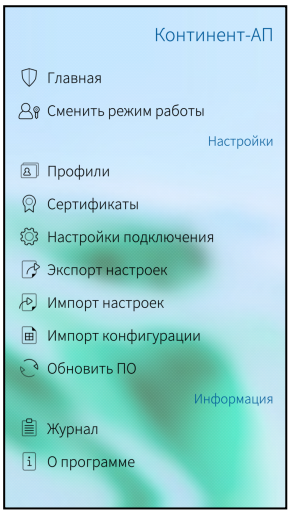
Импорт настроек

Примечание. 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 continentra-settings.csf.

Для импорта настроек:

1. В главном окне приложения откройте меню.



2. Выберите пункт "Импорт настроек".

   Откроется директория внутренней памяти устройства.

3. Выберите в папке файл настроек и нажмите кнопку "Выбрать".

   Приложение настроится автоматически и появится главное окно приложения.

Окно "Профили"

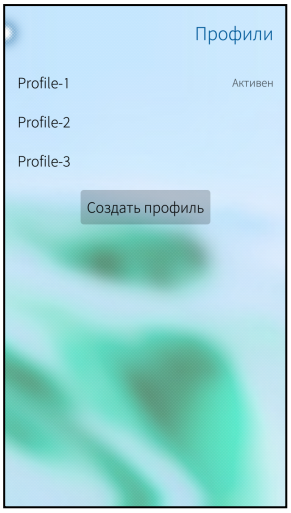
Список профилей

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

Для перехода к списку профилей:

- В главном окне приложения выберите панель "Профиль".

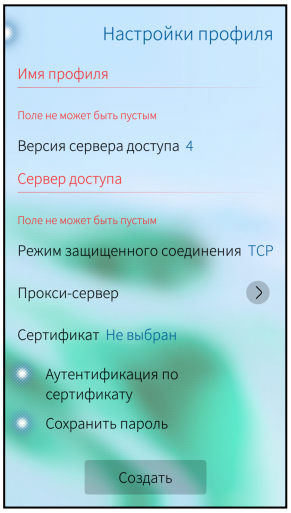
  На экране появится окно "Профили":



Для создания профиля:

1. Нажмите кнопку "Создать профиль" в окне "Профили".

   На экране появится окно:



2. Активируйте поле "Сертификат". В раскрывающемся списке появятся корневые и пользовательские сертификаты. Выберите сертификат. В зависимости от выбранного типа сертификата автоматически заполнится поле "Версия сервера доступа" и установится переключатель "Аутентификация по сертификату".

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

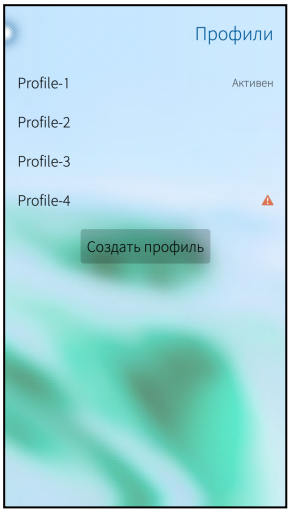
   - если выбран пользовательский сертификат для сервера доступа 4.x, то активируется переключатель "Аутентификация по сертификату". Если деактивировать переключатель "Аутентификация по сертификату", то в поле "Сертификаты" отобразится название корневого сертификата и аутентификация будет производиться по логину и паролю;
   - если выбран пользовательский сертификат для сервера доступа 3.x, то переключатель "Аутентификация по сертификату" активируется и блокируется. Деактивировать его нельзя, доступна аутентификация только по сертификату;
   - если выбран самоподписанный корневой сертификат для сервера доступа 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.

3. Для выбора параметров подключения через прокси-сервер выберите TCP в режиме защищенного соединения, активируйте строку "Прокси-сервер" и в открывшейся группе параметров введите их значения. Нажмите кнопку "Включить".

Примечание. При выборе опции режима защищенного соединения UDP строка "Прокси-сервер" будет деактивирована.

4. Для ввода дополнительных параметров установите отметку в поле "Дополнительно" и введите их значение.
5. Заполните оставшиеся пустыми поля.
6. Нажмите кнопку "Создать".

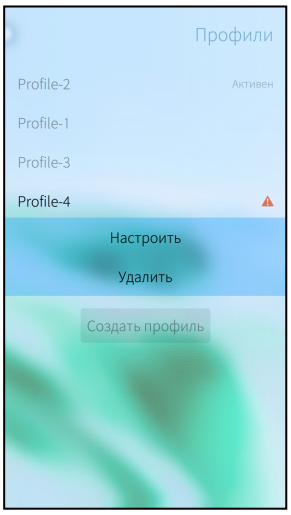
   Профиль появится в окне "Профили".



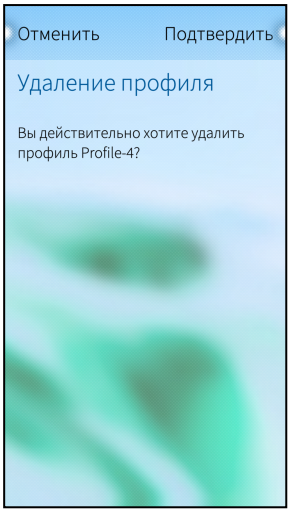
Для удаления профиля:

Примечание. Активный профиль удалить нельзя!

1. В окне "Профили" нажмите и удерживайте нужный профиль. Под профилем появится раскрывающийся список:



2. Нажмите "Удалить". На экране появится сообщение:

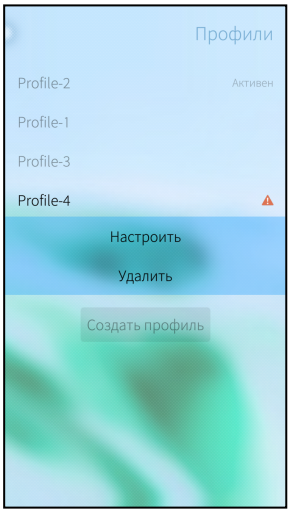


3. Нажмите "Подтвердить". Профиль будет удален.

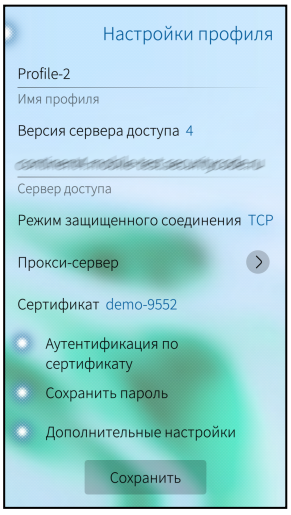
Для настройки профиля:

Примечание. Редактирование профиля запрещено при установленном соединении с сервером доступа.

1. В окне "Профили" нажмите и удерживайте нужный профиль. Под профилем появится раскрывающийся список:



2. Нажмите "Редактировать". На экране появится окно:



3. Внесите исправления в доступные строки и нажмите "Сохранить".

Для смены активного профиля в приложении:

- в окне "Профили" выберите профиль. В перечне профилей он займет первое место и его статус сменится на "Активен".

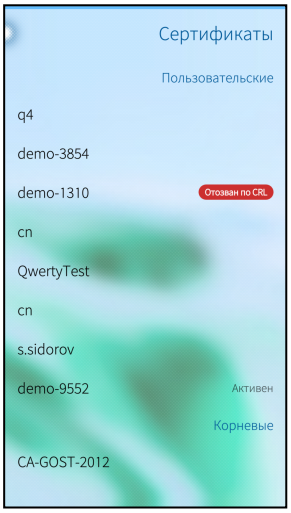
Примечание. Активировать профиль без сертификата нельзя. Профиль без сертификата отмечается восклицательным знаком  .

Окно "Сертификаты"

Описание окна

Для работы с сертификатами:

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

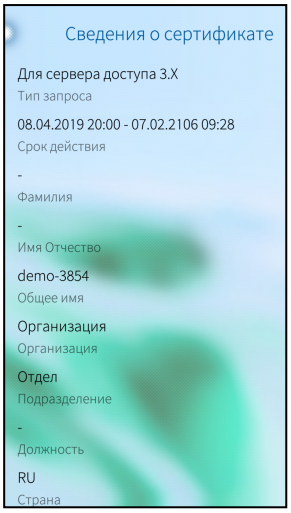


В окне перечислены все импортированные на устройство пользовательские и корневые сертификаты. Актуальное состояние сертификатов отображается на экране рядом с названием сертификата. Для отображения состояния используются следующие отметки:

Отметка	Обозначение
"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 истек
"Нет CRL"	Данный сертификат не прошел проверку по CRL

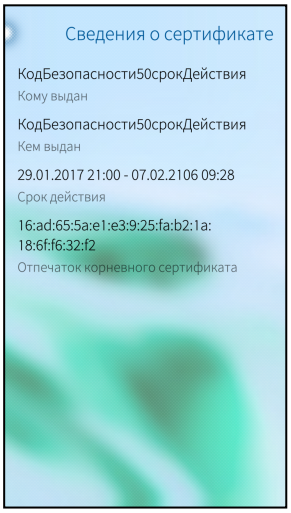
Для просмотра полной информации о пользовательском сертификате:

- выберите его в списке. Окно примет вид:



Для просмотра полной информации о корневом сертификате:

- выберите его в списке. Окно примет вид:



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 из полного набора выберите в списке пользовательский сертификат и удерживайте его. В раскрывающемся списке нажмите кнопку "Корневой сертификат".

Для удаления сертификата:

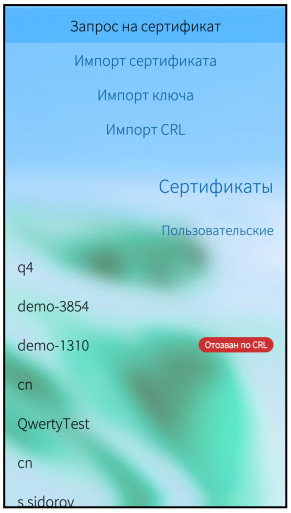
1. В окне "Сертификаты" нажмите и удерживайте нужный сертификат. Под сертификатом появится раскрывающийся список с вариантами действий.
2. Нажмите "Удалить".
3. Нажмите "Подтвердить". Сертификат будет удален.

Дополнительное меню

Запрос на сертификат

Для создания запроса на сертификат:

1. В окне "Сертификаты" выполните скользящее движение вниз до тех пор, пока кнопка "Запрос на сертификат" не будет выделена:



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

2. Введите сведения о пользователе. Для ввода сведений выделите поле и используйте экранную клавиатуру в нижней части окна.

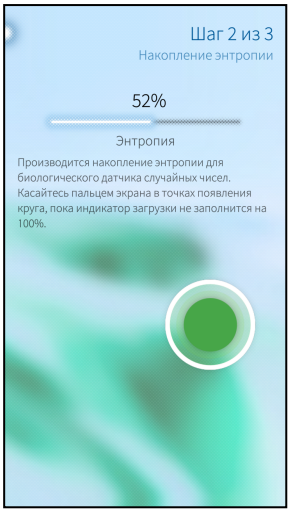
Примечание. Тип запроса зависит от версии сервера доступа.

В зависимости от выбранного типа субъекта являются обязательными следующие поля:

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

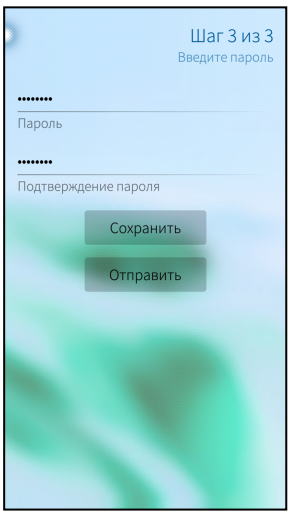
3. После ввода сведений нажмите кнопку "Далее".

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



Пояснение. 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:



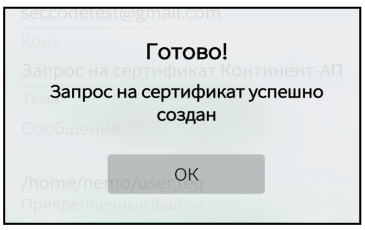
4. Введите и подтвердите пароль.

Примечание. Минимальные требования к паролю:

- длина пароля должна быть не менее 6 символов;
- пароль должен состоять из букв латинского алфавита (A-z), арабских цифр (0-9) и специальных символов (. , : ; ? ! * + % - < > @ [ ] {} / \ _ {} $ # ~ ^ & = ' " ` | №);
- буквенная часть пароля должна содержать как строчные, так и прописные (заглавные) буквы.

5. Нажмите "Отправить".

   На экране появится сообщение:



6. Нажмите "ОК".

   На экране появится директория внутренней памяти устройства.

7. Выберите папку для сохранения и нажмите кнопку "Выбрать".

   Файл запроса и ключевой контейнер будут сохранены в указанной папке.

8. Появится окно отправки письма. Автоматически будут заполнены поля "Тема" и прикреплен файл запроса.

9. Впишите адрес и нажмите кнопку "Отправить".

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

Импорт сертификата

Для импорта сертификата:

1. В окне "Сертификаты" выполните скользящее движение вниз до тех пор, пока кнопка "Импорт сертификата" будет выделена.

   На экране появится директория внутренней памяти устройства.

2. Выберите нужную папку и нажмите кнопку "Выбрать".

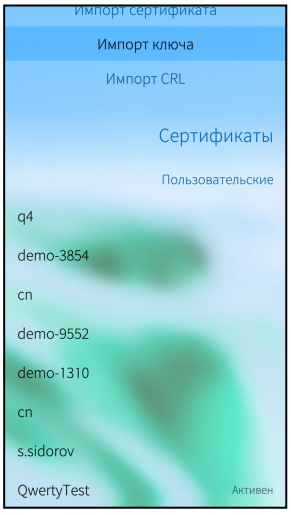
   На экране появится окно "Сертификаты". В списке сертификатов появятся новые пользовательские и корневые сертификаты. Количество и тип сертификатов зависит от набора, переданного администратором.

Импорт ключа

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

Для импорта ключа:

1. Выполните скользящее движение вниз до тех пор, пока кнопка "Импорт ключа" не будет выделена.



   На экране появится директория внутренней памяти устройства.

2. Выберите папку и нажмите кнопку "Выбрать".

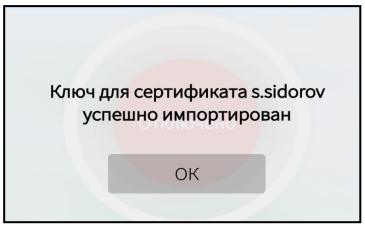
   На экране появится сообщение с инструкцией и индикатором накопления энтропии для биологического датчика случайных чисел. Нажимайте на зеленый круг на экране.

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.

3. Введите пароль, полученный от администратора, и нажмите кнопку "Продолжить".

   Операция будет завершена, и появится сообщение об успешном импорте.



4. Нажмите "ОК".

   В папке сохранится ключ в формате user.key.

Импорт CRL

Администратор безопасности загружает список отозванных сертификатов в виде файла certcrl.crl на сервере доступа "Континент-АП".

Примечание. Перед выполнением операции "Импорт CRL" включите проверку по CRL в настройках подключения.

Для установки списка отозванных сертификатов на мобильном устройстве:

- поместите полученный файл в папку с сертификатами пользователя.

Для импорта CRL:

1. В окне "Сертификаты" выполните скользящее движение вниз до тех пор, пока кнопка "Импорт CRL" не будет выделена.

   На экране появится директория внутренней памяти устройства.

2. Выберите папку и нажмите кнопку "Выбрать".

   На экране появится окно "Сертификаты". Отозванные сертификаты будут помечены как "Отозван по CRL".

Глава 3
Служебные операции

Обновление

Обновление программного обеспечения абонентского пункта выполняется при переходе на новую версию. Для обновления используется rpm-файл, подготовленный компанией-разработчиком.

Предусмотрены два варианта загрузки файла обновления:

- загрузка с внутренней памяти устройства;
- обновление приложения из магазина приложений Jolla.

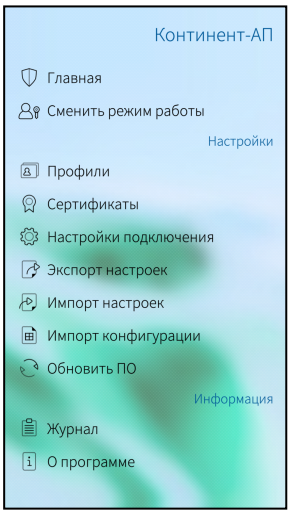
В процессе обновления выполняются проверки:

- обновляемой версии абонентского пункта;
- целостности и аутентичности файла обновления.

Внимание! Перед выполнением процедуры обновления проверьте уровень заряда аккумулятора мобильного устройства. Уровень заряда должен составлять не менее 50% от максимального.

Для обновления программного обеспечения:

1. В главном окне приложения нажмите кнопку вызова меню и выберите пункт "Обновление ПО".



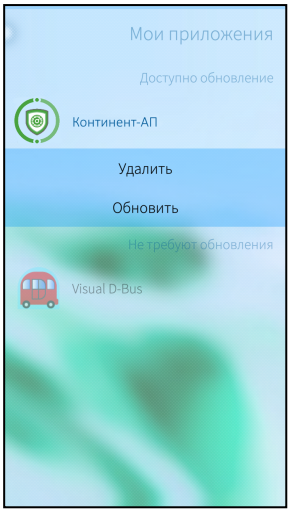
   Появится внутренняя директория устройства.
2. Выберите файл и нажмите кнопку "Выбрать".

   Начнется процедура обновления приложения.
3. Дождитесь завершения обновления приложения "Континент-АП".
4. Проведите контроль целостности (см. стр.**26**).

Для обновления приложения из магазина Jolla:

1. Запустите приложение "Jolla".

   На экране появится страница магазина со сгруппированными по категориям приложениями.
2. Выберите пункт "Мои приложения". В открывшемся перечне приложений выделите пункт "Континент-АП", пока не раскроется список:



3. Нажмите "Обновить".

   Начнется процедура обновления приложения.
4. Дождитесь завершения обновления приложения "Континент-АП".
5. Проведите контроль целостности (см. стр.**26**).

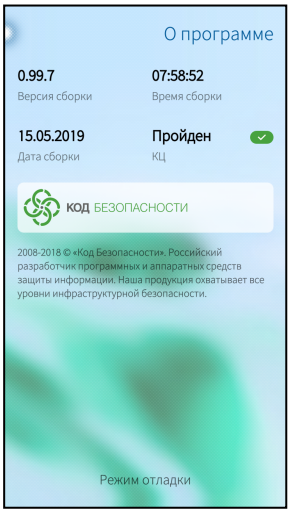
Контроль целостности

Контроль целостности приложения

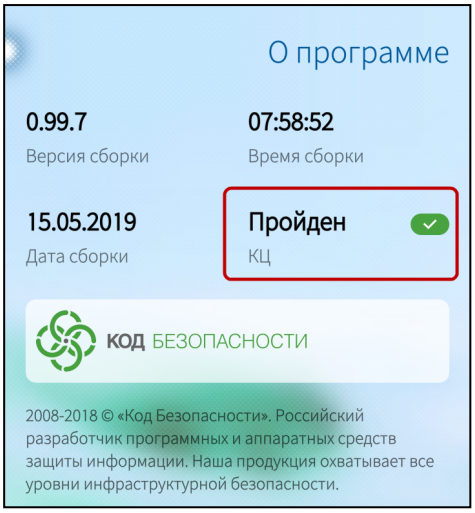
Контроль целостности (далее — КЦ) файлов заключается в сравнении текущих значений контрольных сумм с эталонными значениями контрольных сумм динамических библиотек, заранее вычисленных при установке приложения на устройстве.

Для проведения КЦ приложения:

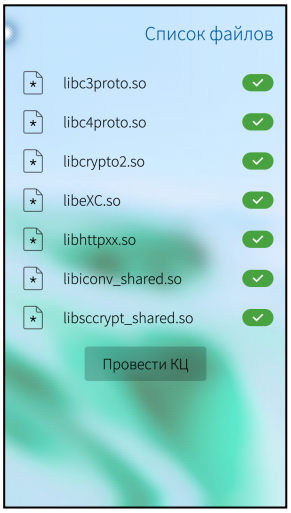
1. В главном окне откройте меню и выберите пункт "О программе".



2. В появившемся окне нажмите на область, указанную на рисунке:



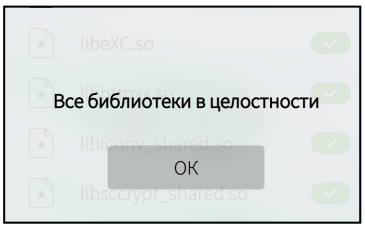
Откроется окно "Список файлов".



3. Нажмите кнопку "Провести КЦ".

   При обнаружении нарушения КЦ работа приложения блокируется, в журнале записывается соответствующее событие.

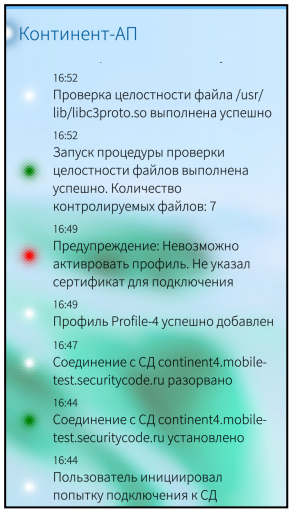
   Если КЦ пройден успешно, появится сообщение:



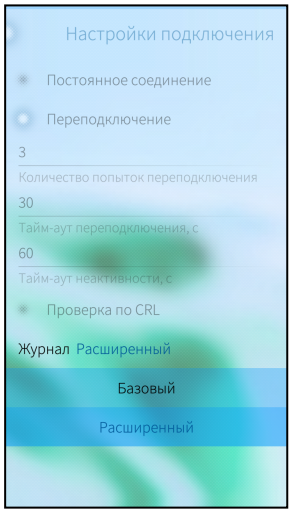
Журнал

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.



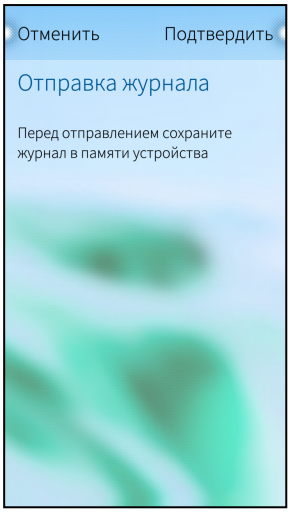
Расширенный уровень детализации включается в разделе "Настройки подключения". Все возможные события, их уровень детализации и цветовое обозначение представлены в таблице ниже.

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

Уровень детализации	Цвет	Событие
Базовый	Черный	Удалена ссылка на папку с корневым сертификатом
Базовый	Зеленый	Соединение с СД установлено
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	Загрузка CRL
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

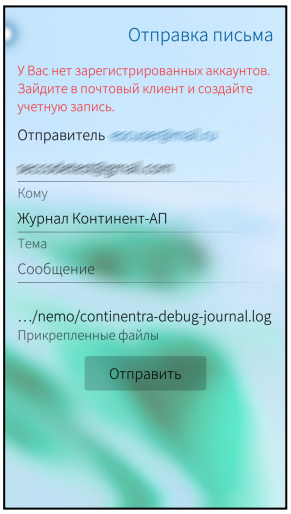
Для отправки журнала в техническую поддержку:

1. В окне "Журнал" нажмите кнопку "Отправить журнал".



2. Нажмите кнопку "Подтвердить". Откроется директория внутренней памяти устройства.
3. Выберите папку и нажмите "Выбрать".

   Файл журнала continentra-journal.log будет создан и сохранен в указанную папку. Появится окно отправки письма. Автоматически будут заполнены строки "Тема" и приложен файл журнала.
4. Нажмите кнопку "Отправить".

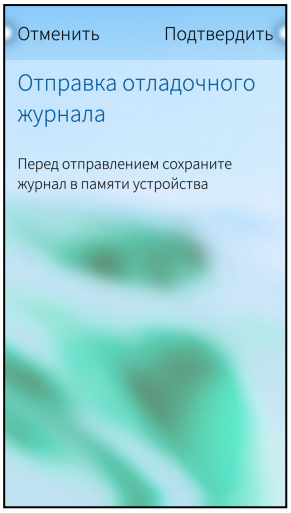


Отладочный журнал

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

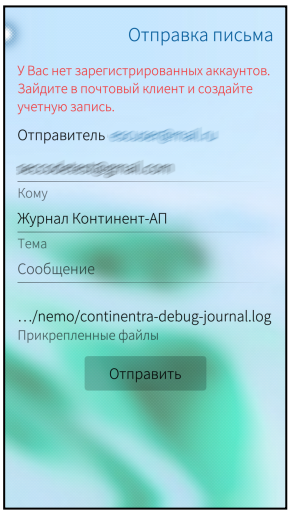
Для отправки журнала в техническую поддержку:

1. В окне "Журнал" нажмите кнопку "Отправить отладочный журнал". Откроется окно:



2. Нажмите кнопку "Подтвердить". Откроется директория внутренней памяти устройства.
3. Выберите папку и нажмите "Выбрать".

   Файл журнала continentra-debug-journal.log будет создан и сохранен в указанную папку. Появится окно отправки письма. Автоматически будут заполнены строки "Тема" и приложен файл журнала.
4. Нажмите кнопку "Отправить".



Управление режимом работы

"Континент-АП" функционирует в двух режимах:

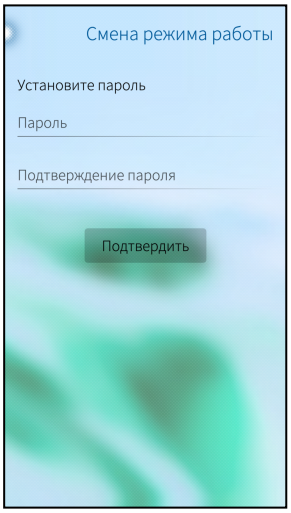
- основной режим (устанавливается по умолчанию) — пользователю предоставляются права полного доступа. Права в основном режиме:
  - подключение и отключение от СД;
  - просмотр списка профилей;
  - активация профиля;
  - просмотр информации о профиле и редактирование;
  - удаление профиля;
  - экспорт/импорт настроек;
  - импорт конфигурации;
  - создание запроса на сертификат;
  - импорт сертификата;
  - просмотр импортированных сертификатов;

  - просмотр сведений о сертификате;
  - импорт ключа;
  - импорт CRL;
  - удаление сертификата;
  - скрытие сертификата во внутренней памяти устройства;
  - просмотр и редактирование настроек подключения;
  - смена режима работы;
  - просмотр и сохранение журнала;
  - обновление приложения;
  - просмотр раздела "О программе";
- частный режим — пользователю "Континент-АП" предоставляются права ограниченного доступа к управлению настройками приложения. Права в частном режиме:
  - подключение и отключение от СД по заранее активированному профилю;
  - просмотр и сохранение журнала;
  - просмотр раздела "О программе".

Для смены режима работы:

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

   На экране появится окно "Установите пароль".



3. Введите пароль блокировки в поля "Пароль", "Подтверждение пароля" и нажмите "Подтвердить".

   На главном экране появится надпись "Включен частный режим" на синем фоне, функции приложения будут ограничены.

Чтобы сменить режим работы, повторите предыдущую операцию еще раз. Если надпись "Включен частный режим" в главном окне приложения пропала, значит — активирован основной режим.