КОД безопасности

Средство криптографической защиты информации

Континент ZTN Клиент для Android

Руководство администратора

АМБС.26.20.40.140.005 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

Список сокращений

АПКШ	Аппаратно-программный комплекс шифрования
КЦ	Контроль целостности
ОС	Операционная система
ПО	Программное обеспечение
СД	Сервер доступа
СКЗИ	Средство криптографической защиты информации
CDP	CRL Distribution Point
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
UUID	Universally unique identifier
VPN	Virtual Private Network
ZTN	Zero Trust Networking

Введение

Документ предназначен для администраторов изделия "Средство криптографической защиты информации "Континент ZTN Клиент для Android" АМБС.26.20.40.140.005 (далее — Континент ZTN Клиент, СКЗИ, приложение). В нем содержатся сведения, необходимые для настройки и эксплуатации СКЗИ "Континент ZTN Клиент для Android".

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 и основные функции

Программное обеспечение СКЗИ реализовано в виде приложения "Континент ZTN Клиент". Приложение устанавливается на мобильные устройства, функционирующие под управлением ОС Android от версии 6.0 до версии 12.

Континент ZTN Клиент реализует следующие основные функции:

- установление защищенного соединения и обмен зашифрованными данными с сервером доступа АПКШ "Континент";
- реализация TLS-аутентификации (в том числе односторонней) на основе технологии открытых ключей (используются сертификаты открытых ключей стандарта X.509 версии 3);
- установление защищенного соединения с TLS-сервером на базе протокола HTTPS и обмен данными с ресурсами корпоративной сети;
- хранение ключевой информации в защищенном контейнере;
- проверка сертификатов ключей по списку отозванных сертификатов;
- очистка сессионной, включая криптографическую, информации при разрыве соединения;
- контроль целостности файлов программного обеспечения;
- регистрация событий, связанных с функционированием приложения.

Континент ZTN Клиент поддерживает возможность работы с серверами, поддерживающими протокол TLS 1.0, 1.2.

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 ZTN Клиент 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;
- формирование и проверка электронной подписи — соответствует ГОСТ Р 34.10-2012;
- расчет хэш-функции — соответствует ГОСТ Р 34.11-2012.

VPN

СКЗИ в режиме VPN позволяет осуществлять установление защищенного соединения и обмен зашифрованными данными с сервером доступа изделий "Аппаратно-программный комплекс шифрования "Континент" версий 3.7, 3.9 (далее — АПКШ "Континент") и узлом безопасности с включенным компонентом "Сервер доступа" изделия "Комплекс безопасности "Континент". Версия 4" (далее — комплекс "Континент") через общедоступные (незащищенные) сети.

СКЗИ поддерживает соединение по протоколам версий 3.X и 4.X:

Протокол версий 3.X	Протокол версий 4.X
Для соединения могут использоваться протоколы TCP или UDP	Для соединения используется протокол TCP
Аутентификация производится с помощью сертификата пользователя	Аутентификация производится с помощью сертификата пользователя или с помощью логина и пароля

TLS

СКЗИ в режиме TLS предназначено для реализации защищенного доступа удаленных пользователей к веб-ресурсам корпоративной сети по каналам связи общих сетей передачи данных с использованием шифрования по ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015.

Для подключения к защищаемым веб-ресурсам корпоративной сети удаленный пользователь должен в адресной строке веб-браузера ввести имя веб-ресурса. По указанному имени Континент ZTN Клиент посылает TLS-серверу запрос на создание защищенного соединения.

На основании принятого запроса TLS-сервер запускает процедуру аутентификации "клиент– сервер". Аутентификация проводится на основе сертификатов открытых ключей.

После успешного завершения процедуры аутентификации выполняется генерация сеансового ключа, и между СКЗИ и TLS-сервером устанавливается защищенное соединение по протоколу TLS. Далее TLS-сервер направляет запрос СКЗИ по указанному пользователем адресу веб-ресурса в защищаемую сеть. Полученный от веб-сервера ответ на запрос TLS-сервер возвращает в рамках защищенного соединения.

В случае невыполнения по каким-либо причинам требований, предъявляемых к аутентификации СКЗИ и TLS-сервера, защищенное соединение не устанавливается и доступ пользователя к веб-ресурсу блокируется.

Сертификаты

Для создания защищенного соединения между СКЗИ и СД пользователь приложения получает у администратора безопасности и устанавливает на мобильном устройстве следующие сертификаты:

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

В зависимости от указаний администратора пользователь получает сертификаты двумя способами:

- Администратор передает пользователю корневой и пользовательский сертификаты вместе с закрытым ключом пользователя, записанным на карте памяти или внешнем носителе.
- По требованию администратора пользователь создает на 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.

Поддерживается работа с ключами форматов PKCS#15, с сертификатами X.509v3 форматов DER и PEM. Также предусмотрена проверка сертификатов по списку отозванных сертификатов.

> **Внимание!** Максимальный срок действия закрытого ключа — 15 месяцев от даты начала срока действия сертификата пользователя. По истечении этого срока работа с сертификатом будет невозможна. Необходимо осуществить перевыпуск сертификата пользователя с закрытым ключом.

Глава 2
Ввод в эксплуатацию

Установка и первый запуск приложения

Установка приложения выполняется пользователем из магазина приложений (например, из Google Play) или с использованием установочного файла с расширением ".apk".

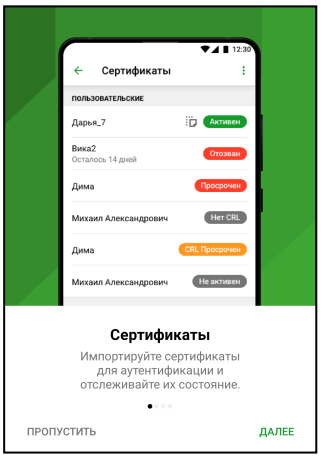
Внимание!

- Для работы с Google Play необходимо наличие учетной записи Google.
- Установочный apk-файл хранится на поставляемом диске. Для установки с использованием apk-файла необходимо перенести файл на требуемое устройство, разрешить на этом устройстве установку приложений из неизвестных источников и запустить установочный файл.

Для установки из магазина приложений и первого запуска:

1. В стандартном магазине приложений найдите приложение "Континент ZTN Клиент" и загрузите его на устройство.
2. Запустите приложение.

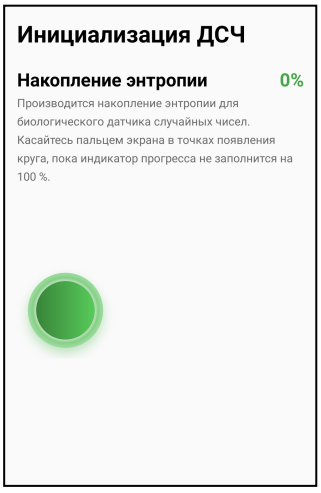
   При первом запуске появятся обучающие экраны.



3. Для просмотра всех обучающих экранов нажимайте кнопку "Далее".
4. На последнем экране нажмите кнопку "Зарегистрироваться".

Примечание. Нажатие кнопки "Пропустить" осуществляет переход к накоплению энтропии.

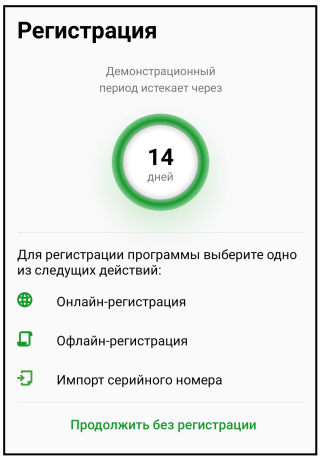
На экране появится сообщение с инструкцией и индикатором накопления энтропии для биологического датчика случайных чисел.



5. Нажимайте на мишень 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 экран регистрации приложения.



Регистрация приложения

Сразу после установки приложение работает в демонстрационном периоде, который составляет 14 дней. Количество дней, оставшихся до окончания демонстрационного периода, отображается в окне "О программе".

Примечание. Функции приложения в демонстрационном периоде не ограничиваются.

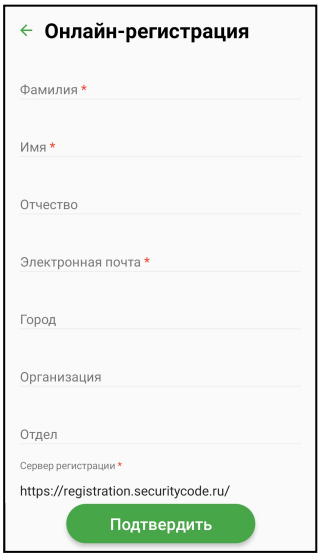
Если по истечении срока демонстрационного периода приложение не зарегистрировано, при каждом запуске будет открываться экран регистрации с соответствующим сообщением. Пропустить регистрацию по истечении этого срока будет невозможно. Экран регистрации также можно вызвать в окне "О программе", нажав на надпись "Демонстрационная версия".

Приложение можно зарегистрировать, выполнив онлайн- или офлайн-регистрацию.

Для онлайн-регистрации:

1. На экране регистрации (см. выше) нажмите кнопку "Онлайн-регистрация".

   Откроется окно ввода данных для регистрации.



2. Введите значения параметров и нажмите кнопку "Подтвердить".

   Начнется процесс регистрации и подключения к указанному серверу регистрации. При успешном завершении операции на экране появится соответствующее сообщение.

3. Нажмите кнопку "ОК".

Для офлайн-регистрации:

1. На экране регистрации (см. стр. **9**) нажмите кнопку "Офлайн-регистрация".

   На экране появится окно ввода данных.

2. Введите значения параметров и нажмите кнопку "Подтвердить".

   Приложение предложит выбрать папку для сохранения файла с регистрационными данными.

3. Выберите нужную папку.

   Файл будет сохранен в указанной папке, и на экране появится сообщение с предложением отправить файл по электронной почте.

4. Нажмите кнопку "ОК".
5. В появившемся окне выберите почтовый клиент для отправки файла.

   Автоматически будут заполнены строки "От", "Тема" и вложен файл.

6. Передайте файл на сервер регистрации для получения файла с серийным номером.
7. После получения файла с серийным номером перенесите его на устройство.
8. Вызовите экран регистрации приложения и нажмите кнопку "Импорт серийного номера".

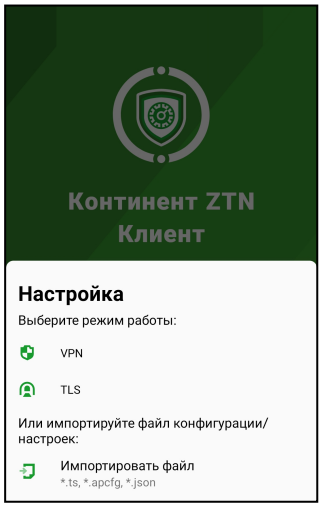
   На экране появится директория внутренней памяти устройства.

9. Откройте папку, содержащую файл с серийным номером, и выберите его.

   При успешном завершении операции на экране появится соответствующее сообщение.

10. Нажмите кнопку "ОК".

Если регистрация выполнена сразу после установки приложения, на экране появится окно предварительной настройки приложения.



После регистрации в окне "О программе" вместо информации о сроке действия демонстрационной версии появится раздел, содержащий регистрационные данные приложения.

Настройка приложения

В зависимости от указаний администратора пользователь настраивает приложение одним из двух способов — импортирует файл конфигурации или настроек либо выполняет ручную настройку.

Для настройки приложения с помощью импорта файла:

1. Администратор передает пользователю файл конфигурации или настроек.
2. Пользователь выполняет импорт файла конфигурации (см. стр. **21**) или настроек (см. стр. **39**).

Для ручной настройки приложения:

1. В зависимости от необходимости пользователь выбирает режим работы приложения — VPN или TLS.
2. Для настройки приложения в VPN-режиме:
   - По требованию администратора пользователь создает на устройстве запрос на сертификат (см. стр. **30**) и передает его администратору.
   - Администратор выпускает корневой и пользовательский сертификаты и передает их пользователю.
   - Пользователь импортирует сертификаты на экране предварительной настройки приложения (см. стр. **10**) и выполняет настройку параметров профиля (см. стр. **17**).

Внимание! Передача файлов сертификатов должна выполняться только по защищенным каналам связи. Передача файлов запросов на сертификаты может выполняться по открытым каналам связи.

3. Для настройки приложения в TLS-режиме:
   - Пользователь выбирает тип соединения — сервер или ресурс, а затем выполняет настройку параметров сервера/ресурса (см. стр. **23**).

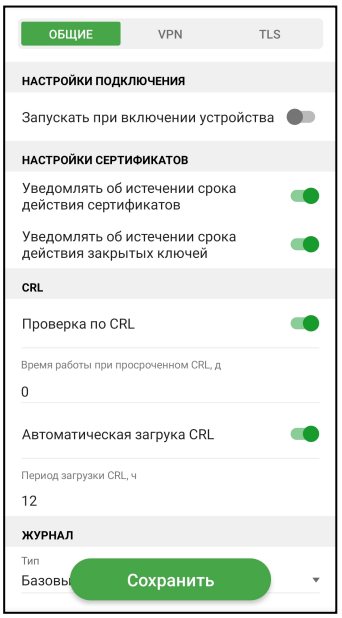
Настройка подключения

Перед подключением к СД или установлением TLS-подключения необходимо настроить параметры подключения.

Для настройки параметров подключения:

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

   На экране появится окно настройки общих параметров подключения.



2. Для настройки параметров режимов работы VPN и TLS перейдите на соответствующие вкладки.
3. Настройте значения параметров (см. стр. **38**) и нажмите кнопку "Сохранить".

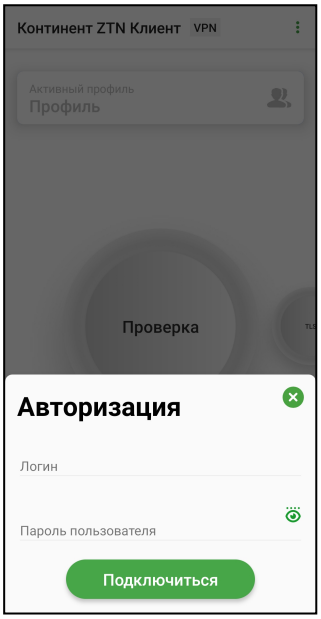
Подключение к серверу доступа

Для подключения к серверу доступа:

1. В главном окне приложения (см. стр. **15**) перейдите на страницу "VPN".
2. Выберите панель "Активный профиль" и активируйте в списке нужный профиль подключения.
3. Нажмите на индикатор подключения.

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

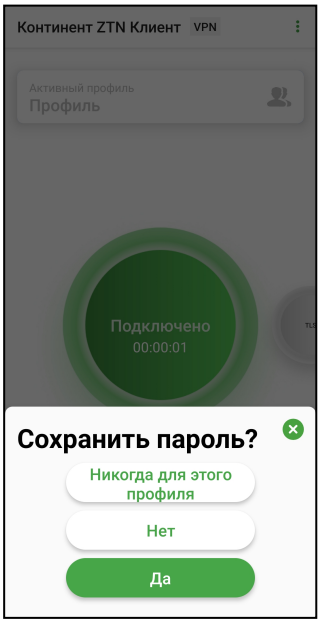
Примечание. В данном примере рассматривается вариант ввода логина и пароля.



4. Введите логин и пароль, а затем нажмите кнопку "Подключиться".

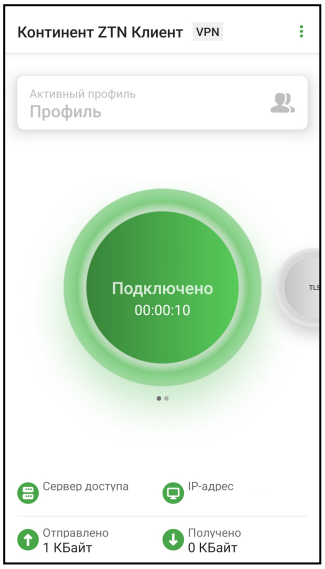
   На экране появится окно запроса на подключение.
5. Нажмите кнопку "ОК".

   Если в настройках профиля переключатель "Сохранить пароль" деактивирован, на экране появится предложение о сохранении пароля.



6. Выполните одно из следующих действий:
   - нажмите кнопку "Да".
     Пароль будет сохранен;
   - нажмите кнопку "Нет".
     Окно закроется, но при следующем подключении появится снова;
   - нажмите кнопку "Никогда для этого профиля".
     Окно закроется и больше появляться не будет.

   Если логин и пароль введены корректно, индикатор подключения изменит цвет на зеленый.



   При активном подключении такие разделы, как "Сертификаты", "CDP", "CRL" и "Настройки", становятся недоступны.

Примечание.
- Раз в полгода необходимо менять пароль ключевого контейнера. При подключении к серверу доступа пользователь аутентифицируется и вводит пароль, происходит проверка и, если срок действия пароля истек, появляется окно, где пользователь должен ввести и подтвердить новый пароль.
- При попытке установления соединения в режиме работы TLS при активном подключении на экране появится предупреждение о том, что текущее соединение будет разорвано.

Подключение к TLS-серверу

Для подключения к TLS-серверу:

1. В главном окне приложения (см. стр. **15**) перейдите на страницу "TLS" и нажмите на индикатор подключения.

   На экране появится сообщение.

2. Нажмите кнопку "OK".
3. В появившемся окне активируйте переключатель для приложения "Континент ZTN Клиент", а затем вернитесь в предыдущее окно.

   На экране появится сообщение о необходимости установки корневого сертификата в хранилище сертификатов устройства.

4. Нажмите кнопку "ОК".

   На экране появится директория внутренней памяти устройства.

5. Выберите папку для сохранения сертификата.

   На экране появится сообщение об успешном сохранении сертификата.

6. Нажмите кнопку "ОК".
7. Перейдите в настройки устройства и затем перейдите по следующему пути: Настройки/Безопасность/Другие параметры безопасности/Установить из памяти.

Примечание. На разных устройствах данный путь может различаться.

8. Выберите пункт "Сертификат СА" и в открывшемся окне нажмите кнопку "Установить в любом случае".
9. Подтвердите выполнение операции.

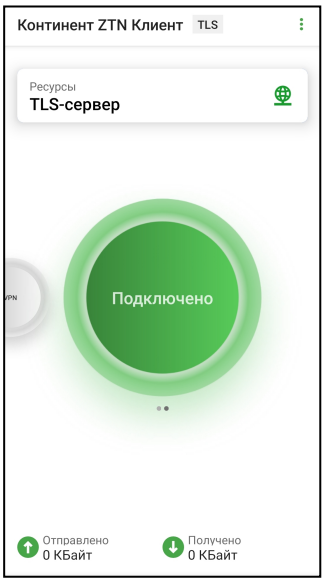
   На экране появится директория внутренней памяти устройства.

10. Выберите в папке сохраненный файл сертификата (см. п. **5**).

    На экране появится уведомление, что сертификат СА установлен.

11. Вернитесь на страницу "TLS" главного окна приложения и нажмите на индикатор подключения.

    Индикатор подключения изменит цвет на зеленый.

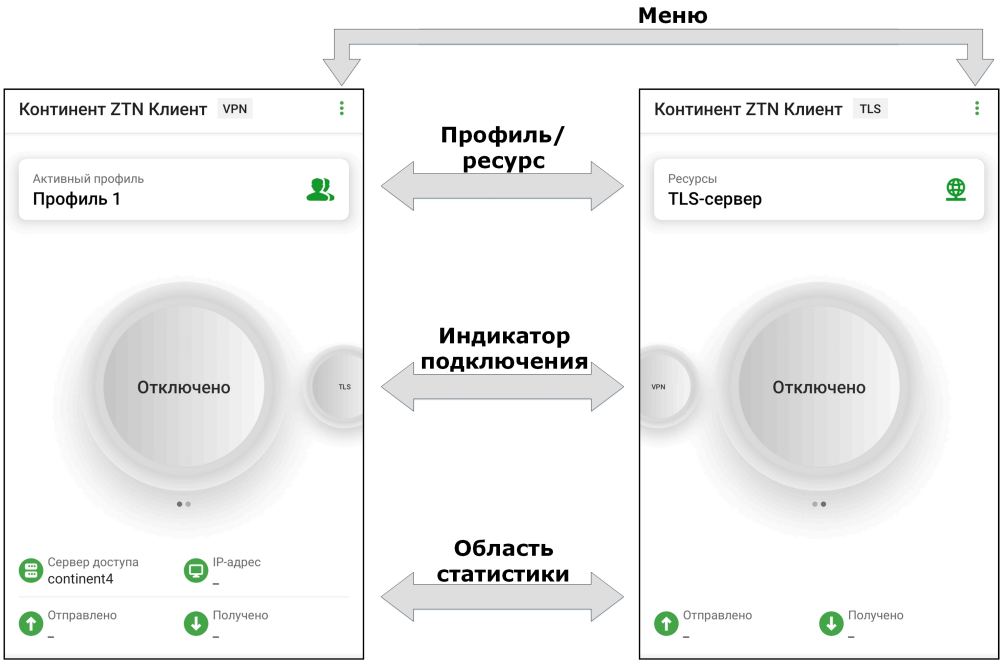


При активном подключении такие разделы, как "Сертификаты", "CDP", "CRL" и "Настройки", становятся недоступны.

Примечание. При попытке установления соединения в режиме работы VPN при активном подключении на экране появится предупреждение о том, что текущее соединение будет разорвано.

Глава 3
Эксплуатация

Главное окно приложения



Описание

Главное окно состоит из следующих объектов:

Объект	Описание
Меню	Разделы для работы с сертификатами, CDP и CRL, настроек подключения, просмотра журналов, смены режима работы и сведений о программе
Активный профиль	Просмотр, создание, настройка и удаление профилей подключения
Ресурсы	Просмотр, добавление, настройка и удаление серверов и ресурсов
Индикатор подключения	Подключение/отключение к/от СД (режим VPN) либо активация режима работы TLS (режим TLS)
Область статистики	Просмотр статистики текущей сессии

Меню главного окна содержит следующие разделы:

Пункт меню	Описание
Сертификаты	Просмотр сведений об импортированных сертификатах, запрос сертификатов, импорт, удаление, а также скрытие во внутренней памяти устройства сертификатов и ключевых контейнеров (см. стр. **27**)
CDP	Добавление, удаление CDP и загрузка CRL (см. стр. **34**)
CRL	Просмотр и редактирование списка CRL, а также импорт CRL (см. стр. **36**)
Настройки	Просмотр и настройка общих параметров подключения, а также параметров режимов VPN и TLS (см. стр. **37**)

Пункт меню	Описание
Сменить режим работы	Переключение режима работы приложения (см. стр. **45**)
Журнал	Сведения о работе приложения (см. стр. **42**)
О программе	Сведения о текущей версии ПО и статусе контроля целостности по результатам проверки контрольных сумм динамических библиотек (см. стр. **41**)

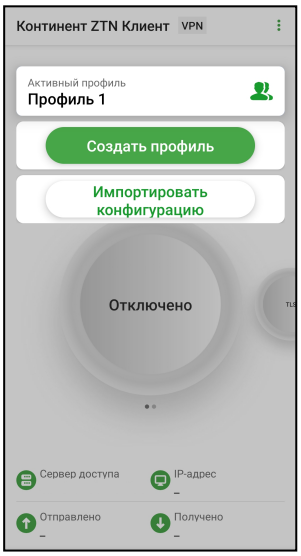
Окно "Профили"

Список профилей

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

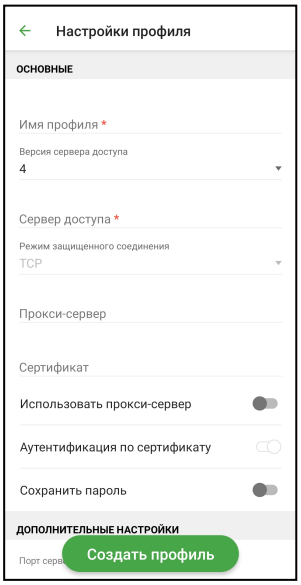
Для перехода к списку профилей:

- В главном окне на странице VPN выберите панель "Активный профиль".
  На экране появится список профилей.



Для создания профиля:

1. В списке профилей нажмите кнопку "Создать профиль".
   На экране появится окно создания профиля.



2. Укажите значения для параметров основных настроек профиля:

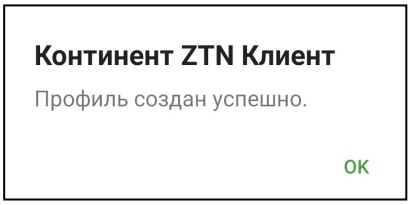
Имя профиля
Название профиля для подключения к СД
Версия сервера доступа
Номер версии СД, к которому будет подключаться пользователь. Поле заполняется автоматически. Если в поле "Сертификат" выбран пользовательский сертификат для СД версий 3.X, версию СД можно изменить на 4. Значение по умолчанию — 4
Сервер доступа
IP-адрес или имя сервера доступа
Режим защищенного соединения
Способ подключения приложения к СД. Может принимать значения: • TCP (стандартное подключение); • UDP (потоковое подключение). Значение по умолчанию — TCP. Для СД версии 3 можно установить значение UDP. Для СД версии 4 режим защищенного соединения всегда TCP
Прокси-сервер
При нажатии на строку параметра открывается окно настройки прокси-сервера. Доступно только при режиме защищенного соединения через TCP. Настройки применяются при условии активации параметра "Использовать прокси-сервер"
Адрес
Сетевое имя или IP-адрес прокси-сервера
Порт
Порт прокси-сервера. Значение по умолчанию — 3128
Аутентификация
Тип аутентификации на прокси-сервере. Значение по умолчанию — "Без аутентификации"
Сертификат
При нажатии на строку параметра открывается окно выбора сертификата, необходимого для подключения. При этом список доступных сертификатов представляет собой список импортированных пользовательских и корневых сертификатов. Если пользователем выбран: • пользовательский сертификат для СД версий 4.X — параметр "Аутентификация по сертификату" активируется. Если его деактивировать, в поле "Сертификат" отобразится название корневого сертификата и аутентификация будет производиться по логину и паролю; • пользовательский сертификат для СД версий 3.X — параметр "Аутентификация по сертификату" активируется и блокируется. Деактивировать его нельзя, доступна аутентификация только по сертификату; • самоподписанный корневой сертификат для СД версий 4.X — параметр "Аутентификация по сертификату" деактивируется и блокируется. Активировать его нельзя, доступна аутентификация только по логину и паролю. При этом логин и пароль администратор передает пользователю по защищенному каналу
Использовать прокси-сервер
Отвечает за использование прокси-сервера. Значение по умолчанию — "ВЫКЛ". Доступно для активации только после настройки параметров в окне "Прокси-сервер"

3. При необходимости укажите значения для параметров дополнительных настроек профиля:

Порт сервера доступа
В зависимости от режима защищенного соединения 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 не получены, их указывают вручную. Адреса, полученные от СД, имеют приоритет над адресами, указанными вручную
Домен
При необходимости можно указать DNS-суффикс, автоматически добавляемый к имени хоста при обращении к защищаемым ресурсам
MTU
Максимальный размер блока (в байт) на канальном уровне сети. Значение по умолчанию — 1500

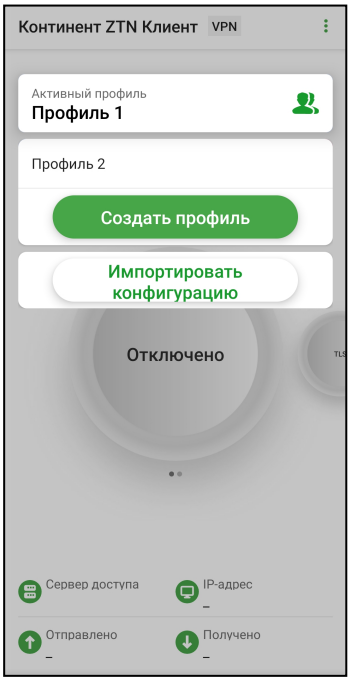
4. Нажмите кнопку "Создать профиль".

   На экране появится сообщение об успешном создании профиля.



5. Нажмите кнопку "ОК".

   Профиль появится в списке.

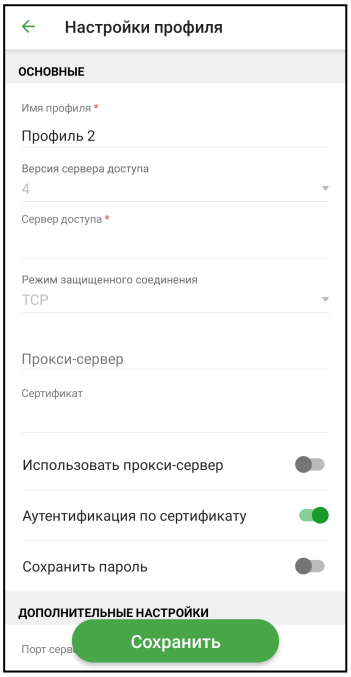


Для настройки профиля:

Примечание. Редактирование профиля запрещено при установленном соединении с СД.

1. В списке профилей проведите пальцем справа налево по профилю.
   Строка профиля примет вид, подобный следующему.

2. Нажмите кнопку  .
   На экране появится окно настройки профиля.



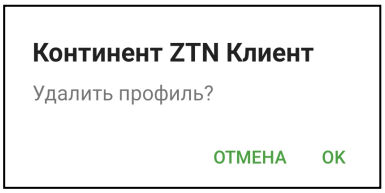
3. Внесите исправления в доступные для редактирования поля.
4. Нажмите кнопку "Сохранить".
   Внесенные в параметры профиля изменения будут применены.

Для удаления профиля:

Внимание! Активный профиль удалить нельзя.

1. В списке профилей проведите пальцем справа налево по профилю.
   Строка профиля примет вид, подобный следующему.

2. Нажмите кнопку  .
   На экране появится запрос на удаление профиля.



3. Нажмите кнопку "ОК".

Для смены активного профиля:

- В списке профилей выберите нужный профиль.

  Выбранный профиль отобразится на панели "Активный профиль".

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

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

Набор компонентов файла конфигурации зависит 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 СД, на котором он был сформирован:

Сервер доступа версий 3.X	Сервер доступа версий 4.X
Всегда зашифрован	Шифрование опционально
Энтропия набирается на устройстве	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 файла конфигурации.

Импорт конфигурации для быстрого старта

Для импорта конфигурации:

1. Администратор формирует файл конфигурации и передает пользователю по электронной 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, регистрирует свою копию СКЗИ (или начинает работу в демонстрационном режиме) и нажимает кнопку "Импортировать файл" на экране предварительной настройки приложения.
4. Пользователь выбирает файл конфигурации, содержащийся на устройстве.
5. Приложение определяет тип конфигурации. Если файл сформирован на СД версий 3.X, на экране появится окно с накоплением энтропии. Если файл сформирован на СД версий 4.X, шаг с накоплением энтропии пропускается.
6. При необходимости пользователь вводит пароль от конфигурации.
7. Пользователь вводит пароль от ключевого контейнера, так как ключ импортируется из конфигурации и конвертируется в формат для СКЗИ.

   Примечание. В состав файла конфигурации может входить несколько ключевых контейнеров. Пользователь должен ввести пароль для каждого ключевого контейнера в наборе.

   Сертификаты и ключевой контейнер извлекаются в скрытую папку. Новые сертификаты импортируются в раздел "Сертификаты", и создаются новые профили. Активным становится профиль с признаком по умолчанию.
8. На экране появляется сообщение об успешном импорте конфигурации, и пользователь нажимает кнопку "ОК".

   Континент ZTN Клиент отображает главный экран приложения с новым активным профилем.

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>-n, а старый профиль останется. При этом значение "n" представляет собой порядковый номер профиля, импортированного повторно.

Импорт конфигурации для обновления сертификатов

Для импорта конфигурации:

1. Администратор формирует файл конфигурации и передает пользователю по электронной 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, выбирает панель "Активный профиль", а затем нажимает кнопку "Импортировать конфигурацию".
4. Пользователь выбирает файл конфигурации, содержащийся на устройстве.
5. 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 СКЗИ.

   Примечание. В состав файла конфигурации может входить несколько ключевых контейнеров. Пользователь должен ввести пароль для каждого ключевого контейнера в наборе.

   Сертификаты и ключевой контейнер извлекаются в скрытую папку. Сертификаты импортируются в раздел "Сертификаты".
7. На экране появляется сообщение об успешном импорте конфигурации, и пользователь нажимает кнопку "ОК".

Континент ZTN Клиент отображает главный экран приложения.

При совпадении имен существующего и импортируемого сертификатов:

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

Если пользователь произведет импорт такой конфигурации с экрана предварительной настройки приложения, для его полной настройки 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 электронной 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, выбирает панель "Активный профиль", а затем нажимает кнопку "Импортировать конфигурацию".
4. Пользователь выбирает файл конфигурации, содержащийся на устройстве.
5. При необходимости пользователь вводит пароль от конфигурации.
6. Приложение 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".
7. Пользователь делает запрос на сертификат и импортирует полученные сертификаты в разделе "Сертификаты".
8. Пользователь редактирует импортированный профиль, привязывает сертификат к новому профилю и нажимает кнопку "Сохранить".
9. На экране появляется сообщение об успешном импорте конфигурации, и пользователь нажимает кнопку "ОК".

   Континент ZTN Клиент отображает главный экран приложения с новым активным профилем.

Если пользователь производит импорт конфигурации с помощью экрана загрузки, появляется сообщение об ошибке: "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 предварительной настройки приложения и отправляет администратору.
2. Администратор на основе запроса формирует файл конфигурации и передает пользователю по электронной 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 и нажимает кнопку "Импортировать файл" на экране предварительной настройки приложения.
5. Пользователь выбирает файл конфигурации, содержащийся на устройстве.
6. При необходимости пользователь вводит пароль от конфигурации.
7. Пользователь выбирает на устройстве папку, которая была сформирована при запросе на сертификат.

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

Из файла конфигурации извлекается информация о сертификате и настройках профиля. Новые сертификаты импортируются в раздел "Сертификаты", и создается новый профиль. Сертификат, соответствующий запросу, и ключевой контейнер привязываются к профилю автоматически. Созданный профиль становится активным после установки настроек.

8. На экране появляется сообщение об успешном импорте конфигурации, и пользователь нажимает кнопку "ОК".

   Континент ZTN Клиент отображает главный экран приложения.

Пользователь также может импортировать конфигурацию, нажав кнопку "Импортировать конфигурацию" на панели "Активный профиль". 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 будут восстановлены.

Окно "Ресурсы"

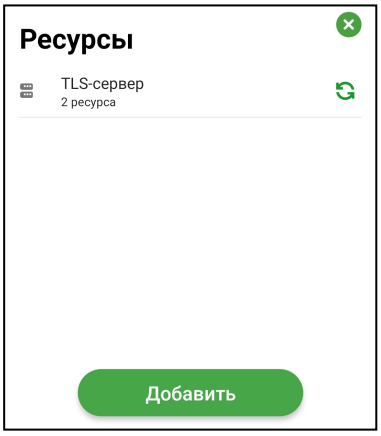
Список ресурсов

Примечание. Настройка списка ресурсов доступна только при неактивном TLS-режиме.

Для перехода к списку ресурсов:

- В главном окне приложения на странице TLS выберите панель "Ресурсы".

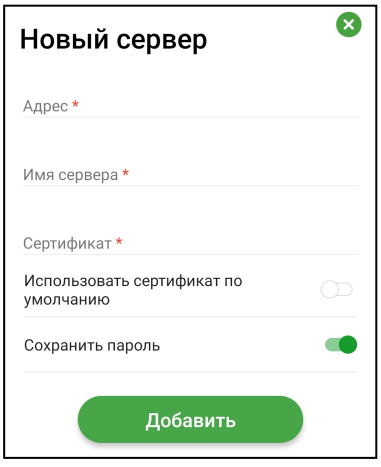
  На экране появится список серверов и ресурсов.



Для добавления сервера:

1. В окне "Ресурсы" нажмите кнопку "Добавить", а затем — кнопку "Сервер".

   Откроется окно добавления сервера.



2. Укажите значения параметров настроек сервера:

Адрес
Сетевое имя или IP-адрес сервера
Имя сервера
Название сервера для установления TLS-подключения
Сертификат
При нажатии на строку параметра открывается окно выбора сертификата, необходимого для подключения. Список доступных сертификатов представляет собой список импортированных пользовательских сертификатов. Если выбран сертификат, указанный в настройках TLS в качестве сертификата по умолчанию, параметр "Использовать сертификат по умолчанию" активируется. Если параметр "Использовать сертификат по умолчанию" ранее был активирован, при выборе другого сертификата в поле "Сертификат" он будет деактивирован
Использовать сертификат по умолчанию
Отвечает за использование сертификата по умолчанию. При активации параметра имя выбранного сертификата по умолчанию появится в поле "Сертификат". Значение по умолчанию — "ВЫКЛ". Доступно для активации после добавления пользовательского сертификата в настройках режима работы TLS (см. стр. **39**)
Сохранить пароль
Отвечает за сохранение пароля при подключении к TLS-серверу. Значение по умолчанию — "ВКЛ". При активации параметра после ввода пароля он будет сохранен, окно запроса пароля больше появляться не будет

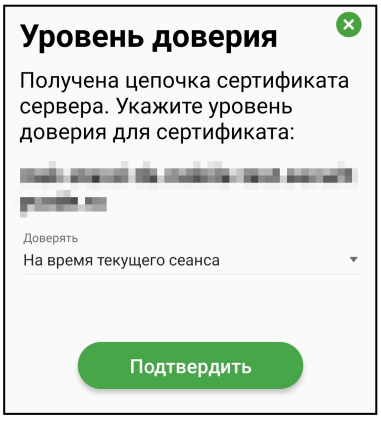
3. Нажмите кнопку "Добавить".
4. Введите пароль ключевого контейнера и нажмите кнопку "Подтвердить".

   На экране появится сообщение об успешном добавлении сервера.

5. Нажмите кнопку "ОК".

Примечание.
- Если первичное установление соединения с Сервером не будет выполнено из-за его недоступности, в строке с ним появится статус "Недоступен" и он будет отмечен как неактивный.
- Если обновление Сервера не будет выполнено, в строке с ним появятся надпись "Требуется обновление" и значок ⚠. Просмотр ресурсов Сервера будет невозможен.

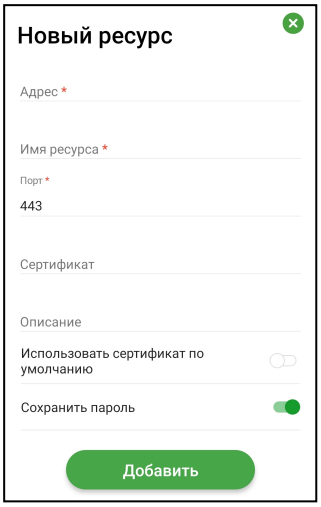
Новый сервер появится в списке, и откроется окно, подобное следующему.



6. Выберите из раскрывающегося списка уровень доверия для сертификата.
7. Нажмите кнопку "Подтвердить".

Для добавления ресурса:

1. В окне "Ресурсы" нажмите кнопку "Добавить", а затем — кнопку "Ресурс". Откроется окно добавления ресурса.

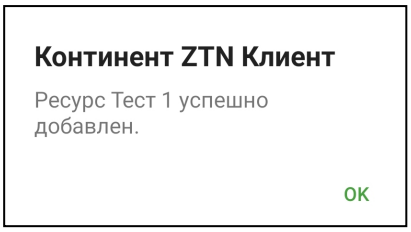


2. Укажите значения параметров настроек ресурса:

Адрес
Сетевое имя или IP-адрес ресурса
Имя ресурса
Название ресурса для установления TLS-подключения
Порт
Номер порта, используемого для установления TLS-подключения. Значение по умолчанию — 443
Сертификат
При нажатии на строку параметра открывается окно выбора сертификата, необходимого для подключения. Список доступных сертификатов представляет собой список импортированных пользовательских и корневых сертификатов. Если выбран сертификат, добавленный в настройках TLS-подключения в качестве сертификата по умолчанию, параметр "Использовать сертификат по умолчанию" активируется. Если параметр "Использовать сертификат по умолчанию" ранее был активирован, при выборе другого сертификата в поле "Сертификат" этот параметр деактивируется
Использовать сертификат по умолчанию
Отвечает за использование сертификата по умолчанию. При активации параметра имя сертификата по умолчанию появится в поле "Сертификат". Значение по умолчанию — "ВЫКЛ". Доступно для активации только после добавления пользовательского сертификата в настройках режима работы TLS (см. стр. **39**)
Сохранить пароль
Отвечает за сохранение пароля при подключении к TLS-серверу. Значение по умолчанию — "ВКЛ". При активированном параметре после ввода пароля он будет сохранен, окно запроса пароля больше появляться не будет

3. Нажмите кнопку "Добавить".
4. При необходимости введите пароль ключевого контейнера и нажмите кнопку "Подтвердить".

На экране появится сообщение об успешном добавлении ресурса.



5. Нажмите кнопку "OK".

   Новый ресурс появится в списке.

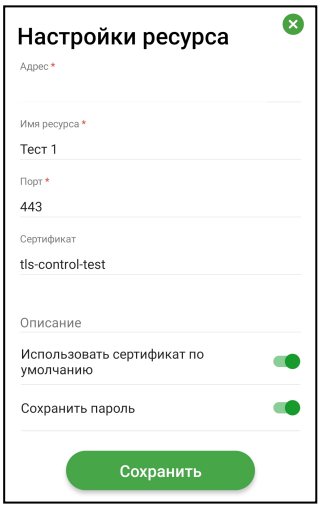
Для настройки сервера/ресурса:

1. В окне "Ресурсы" проведите пальцем справа налево по серверу/ресурсу.

   Строка сервера/ресурса примет вид, подобный следующему.

2. Нажмите кнопку  .

   На экране появится окно редактирования сервера/ресурса.



3. Внесите необходимые исправления и нажмите кнопку "Сохранить".

Для ручного обновления списка ресурсов:

Примечание. В окне "Настройки" на вкладке "TLS" для списка ресурсов по умолчанию активирован переключатель "Автоматическое обновление".

- В окне "Ресурсы" в строке с нужным сервером нажмите кнопку  , а затем, при необходимости, введите пароль для ключевого контейнера.

  В области уведомлений устройства появится сообщение о результате выполнения операции, в случае успеха ресурсы сервера будут обновлены.

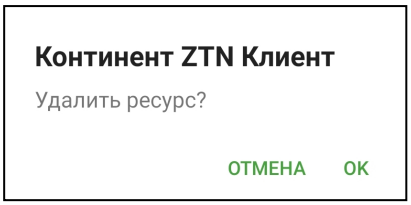
Для удаления сервера/ресурса:

1. В окне "Ресурсы" проведите пальцем справа налево по серверу/ресурсу.

   Строка сервера/ресурса примет вид, подобный следующему.

2. Нажмите кнопку  .

На экране появится запрос на удаление ресурса.



3. Нажмите кнопку "ОК".

   Сервер/ресурс будет удален.

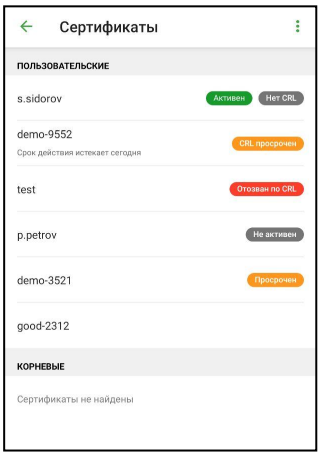
Окно "Сертификаты"

Описание окна

Для работы с сертификатами:

- В главном окне приложения вызовите меню и нажмите кнопку "Сертификаты".

  Откроется окно "Сертификаты".



Примечание.

- При использовании сертификатов для СД версий 3.X проверка по CRL не осуществляется. Если проверка по CRL включена, такие сертификаты будут иметь статус "Нет CRL".
- Если у сертификата отсутствует статус — сертификат не просрочен и прошел проверку по CRL либо проверка по CRL отключена.

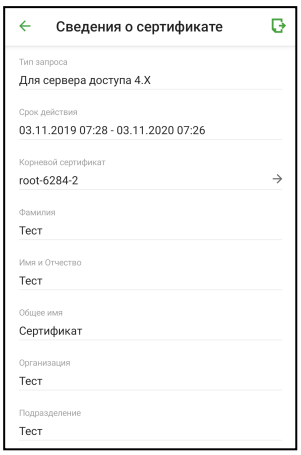
Окно содержит список всех импортированных на устройство пользовательских и корневых сертификатов. Актуальное состояние отображается в виде статусов в строке с названием сертификата. Для отображения состояния используются следующие статусы:

Статус	Значение
Активен	Сертификат актуален и используется устройством в данный момент
Срок действия истекает через n дней	Предупреждение появляется за 14 дней до окончания срока действия сертификата. Переменная n обозначает количество дней
Просрочен	Срок действия сертификата истек
Неактивен	Срок действия сертификата еще не начался
Отозван	Сертификат находится в списке отозванных сертификатов
CRL просрочен	Срок действия CRL истек или еще не начался
Нет CRL	Сертификат не прошел проверку по CRL, так как CRL-файл не импортирован

Для просмотра сведений о пользовательском сертификате:

- Выберите его в списке.

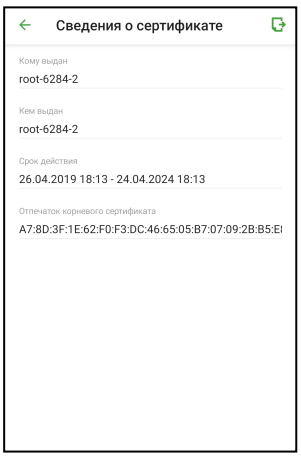
  На экране появятся сведения о сертификате.



Для просмотра сведений о корневом сертификате:

- Выберите его в списке.

  На экране появятся сведения о сертификате.



Примечание. Корневые сертификаты бывают двух видов:

- из полного набора, связанные с пользовательским сертификатом;
- самоподписанные.

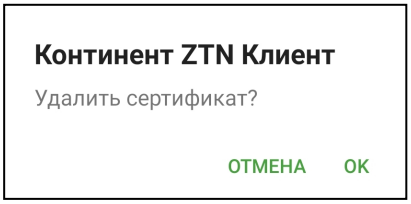
В окне "Сертификаты" отображаются пользовательские и самоподписанные корневые сертификаты. Для просмотра информации о корневом сертификате, который связан с пользовательским, в окне "Сведения о сертификате" нажмите кнопку "Корневой сертификат".

Для удаления сертификата:

Внимание! Сертификат, привязанный к профилю , удалить нельзя.

1. В окне "Сертификаты" проведите пальцем справа налево по строке с сертификатом.
2. Нажмите кнопку  .

   На экране появится запрос на удаление сертификата.



3. Нажмите кнопку "ОК".

   Сертификат будет удален.

Для экспорта сертификата:

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

1. В окне "Сертификаты" нажмите на строку с сертификатом.

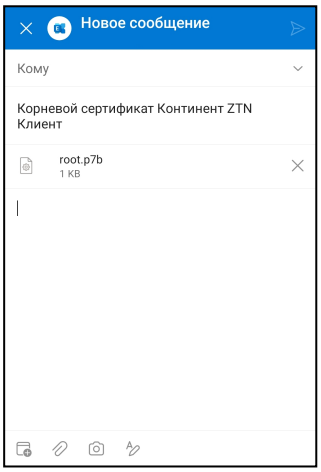
   Откроется окно со сведениями о сертификате.

2. Нажмите кнопку  .

3. В появившемся окне выберите почтовый клиент для отправки сертификата.

   В окне почтового клиента автоматически будут заполнены строки "От", "Тема" и вложен файл сертификата.

   Примечание. В данном примере рассматривается почтовый клиент Microsoft Outlook.



4. Введите адрес получателя и отправьте письмо.

Скрытие сертификатов

Процедура предназначена для защиты файлов от несанкционированных изменения, удаления или передачи. После выполнения процедуры при открытии на устройстве папки, в которой хранятся сертификаты и ключевой контейнер, файлы "user.cer", "root.p7b" и "user.key" будут невидимы для пользователя, в том числе при подключении к компьютеру.

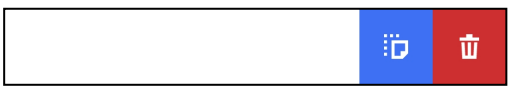
Примечание.

- При импорте файла конфигурации или настроек, а также файла сертификата или архива с сертификатами все сертификаты импортируются скрытыми.
- Если на момент удаления приложения файлы сертификатов или ключей будут скрыты, они будут удалены вместе с приложением.

Для скрытия файлов:

1. Откройте окно "Сертификаты".
2. Проведите пальцем справа налево по строке требуемого сертификата.

   Строка сертификата примет вид, подобный следующему.



3. Нажмите кнопку  .

   Рядом со скрытыми сертификатами появится значок  .

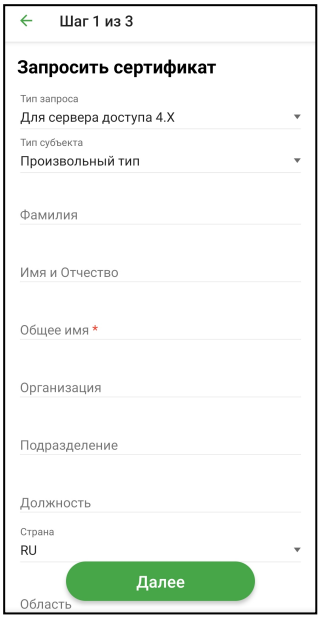
Чтобы отменить процедуру скрытия файлов, выполните ее еще раз и укажите пустую директорию для сохранения файла.

Меню окна "Сертификаты"

Запрос на сертификат

Для создания запроса на сертификат:

1. Вызовите меню в окне "Сертификаты" и нажмите кнопку "Запросить сертификат".



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

2. Введите сведения о пользователе.

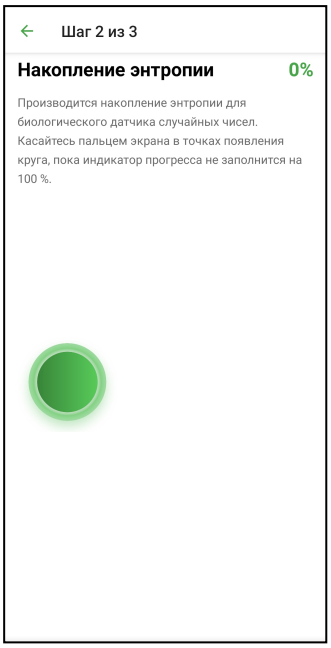
   Примечание. Тип запроса зависит от версии СД.

   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 кнопку "Далее".

   На экране появится окно накопления энтропии.



4. Нажимайте на мишень.

   Примечание. Непопадание по мишени может привести к снижению уровня накопленной энтропии и повторному выполнению операции.

   Когда индикатор покажет 100 %, откроется окно 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 кнопку "Далее".

В нижней части экрана появится меню.

7. Нажмите кнопку "Отправить".

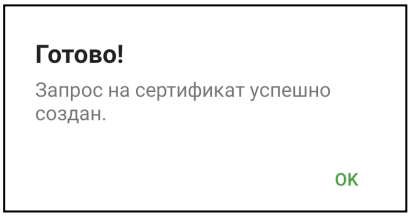
   На экране появится запрос на сохранение файла.

8. Нажмите кнопку "ОК".

   На экране появится директория внутренней памяти устройства.

9. Выберите папку для сохранения запроса на сертификат и нажмите кнопку "Выбрать".

   Файл запроса и ключевой контейнер будут сохранены в указанной папке. На экране появится сообщение об успешном создании запроса.



10. Нажмите кнопку "ОК".
11. В появившемся окне выберите почтовый клиент для отправки письма.

    В окне почтового клиента автоматически будут заполнены строки "От", "Тема" и вложен файл запроса на сертификат.

12. Впишите адрес и отправьте письмо администратору.

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

Импорт сертификатов и ключа

Пользователь имеет возможность импортировать сертификат пользователя, корневой сертификат, ключевой контейнер или архив с сертификатами.

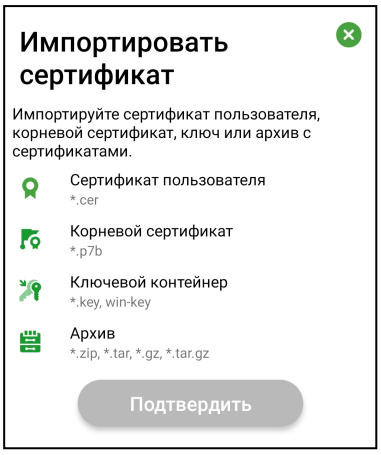
Операция импорта ключа предназначена для случая, когда администратор формирует файлы, включая ключ, без запроса на сертификат. Для корректной работы СКЗИ пользователь должен конвертировать ключ в формат для мобильного приложения "Континент ZTN Клиент". Если ключ не конвертировать, подключение к СД осуществляться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

Для импорта корневого сертификата:

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

1. Вызовите меню в окне "Сертификаты" и нажмите кнопку "Импортировать сертификат".

На экране появится окно импорта сертификатов и ключа.



2. Выберите пункт "Корневой сертификат" или "Архив".

   На экране появится директория внутренней памяти устройства.
3. Выберите файл сертификата или архив, содержащий этот файл.
4. Нажмите кнопку "Подтвердить".

Примечание. При импорте файла сертификата или архива с сертификатами все сертификаты импортируются скрытыми.

На экране появится сообщение об успешном импорте сертификатов.

5. Нажмите кнопку "ОК".

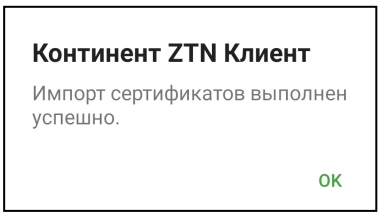
Для импорта пользовательского сертификата и ключа:

Примечание.

- Импорт пользовательского сертификата и ключа необходимо выполнять вместе с корневым сертификатом. Если не выбран пункт "Корневой сертификат", кнопка "Подтвердить" будет неактивной. Если выбраны пункт "Корневой сертификат" и один из пунктов "Сертификат пользователя" и "Ключевой контейнер", будет импортирован только корневой сертификат.
- При импорте архива с сертификатами из почты убедитесь, что внутри архива нет других папок.

1. Вызовите меню в окне "Сертификаты" и нажмите кнопку "Импортировать сертификат".
2. В появившемся окне выполните одно из следующих действий:
   - выберите пункт "Корневой сертификат" и в появившемся окне выберите файл сертификата. Затем повторите действие, выбрав пункты "Сертификат пользователя" и "Ключевой контейнер";
   - либо выберите пункт "Архив" и в появившемся окне выберите архив, содержащий файлы сертификатов и ключа.
3. Нажмите кнопку "Подтвердить".

   На экране появится сообщение об успешном импорте файлов.



4. Нажмите кнопку "ОК".

Примечание. При импорте сертификатов из архива отдельная папка не создается, файлы сертификатов распаковываются в директорию, в которой находится архив.

После выполнения операции импорта на экране появится окно "Сертификаты". В списке появятся новые пользовательские и корневые сертификаты. Количество и тип сертификатов зависят от набора, переданного администратором.

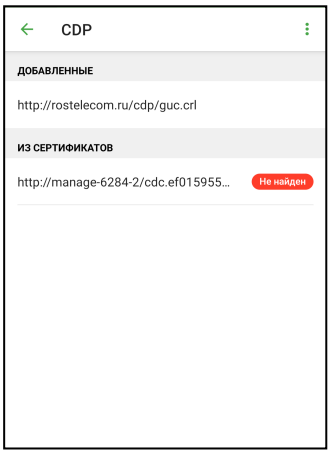
Окно "CDP"

Приложение позволяет в автоматическом или ручном режиме получать CDP, автоматически скачивать CRL для проверки валидности используемых сертификатов, а также вручную импортировать CRL.

Для управления CDP:

- В главном окне приложения вызовите меню и нажмите кнопку "CDP".

  Откроется окно "CDP".



Управление CDP

Если используемые сертификаты содержат информацию о CDP, приложение получит ее при импорте сертификатов (см. стр. **32**).

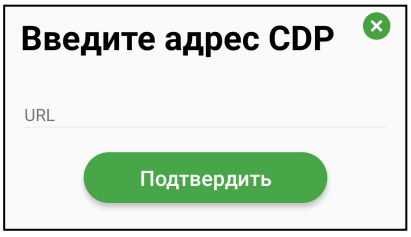
Примечание. Для сертификатов, выпущенных на СД, CRL не требуется. Для подключения к СД отключите проверку по CRL (см. стр. **38**).

Если импортированные сертификаты не содержат CDP, необходимо вручную добавить CDP в список.

Для добавления CDP вручную:

1. Вызовите меню в окне "CDP" и нажмите кнопку "Добавить CDP".

   Появится окно для ввода URL-адреса.



2. В поле "URL" введите адрес CDP в формате:

   ```
   http://[link].crl
   ```

   где [link] — доменное имя требуемого ресурса.

3. Нажмите кнопку "Подтвердить".

   Новый CDP будет добавлен в список.

Для удаления CDP из списка:

Примечание.
- CDP, полученные из сертификатов, нельзя удалить вручную. Такие CDP удаляются автоматически после удаления всех сертификатов, из которых они были получены.
- CRL, загруженные из CDP, не будут удалены при удалении этого CDP. CRL можно удалить вручную в окне "CRL".

1. В окне "CDP" проведите пальцем справа налево по строке с CDP.
   Строка CDP примет вид, подобный следующему.

2. Нажмите кнопку  .
   На экране появится сообщение с запросом на подтверждение операции.
3. Нажмите кнопку "OK".
   CDP будет удален из списка.

Для изменения URL-адреса CDP:

Примечание. CDP, полученные из сертификатов, не могут быть изменены.

1. В окне "CDP" проведите пальцем справа налево по строке с CDP.
   Строка CDP примет вид, подобный следующему.

2. Нажмите кнопку  .
   На экране появится окно, содержащее URL-адрес выбранного CDP.
3. В поле "URL" внесите требуемые изменения.
   URL-адрес CDP должен быть представлен в следующем формате:
   ```
   http://[link].crl
   ```
   где [link] — доменное имя требуемого ресурса.
4. Нажмите кнопку "Подтвердить".
   Адрес CDP будет изменен.

Загрузка CRL

Автоматическая загрузка CRL происходит следующими способами:
- в результате добавления CDP после импорта сертификатов;
- согласно расписанию в окне "Настройки" (см. стр. **38**);
- при каждом запуске приложения.

Внимание!
- Если для CDP не был найден CRL, в строке с этим CDP появится статус "Не найден".
- Если CRL просрочен, в строке с соответствующим CDP появится статус "Устарел".

Для загрузки CRL вручную:

Примечание. Операция позволяет обновить сразу весь список CRL.

- Вызовите меню в окне "CDP" и нажмите кнопку "Скачать CRL".
  При успешной загрузке CRL в области уведомлений устройства появится соответствующее сообщение.

Окно "CRL"

Континент ZTN Клиент позволяет выполнять следующие операции со списками отозванных сертификатов:

- импорт CRL;
- просмотр сведений о CRL;
- экспорт CRL по электронной почте;
- удаление CRL.

Для управления CRL:

- В главном окне приложения вызовите меню и нажмите кнопку "CRL".

  Откроется окно "CRL".

  Примечание. В случае если срок CRL истек или еще не начался, в строке с ним появится статус "Просрочен".

Для импорта файла CRL:

1. Вызовите меню в окне "CRL" и нажмите кнопку "Импортировать CRL".

   На экране появится директория внутренней памяти устройства.
2. Выберите папку, содержащую файл.

   После успешного завершения операции на экране появится соответствующее сообщение.
3. Нажмите кнопку "ОК".

Для просмотра сведений о CRL:

- В окне "CRL" выберите нужную строку из списка.

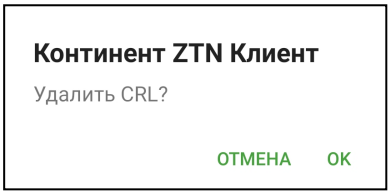
  На экране появится окно со сведениями о CRL.

Для отправки файла CRL:

1. В окне "CRL" выберите нужную строку из списка.
   Откроется окно "Сведения о CRL".
2. Нажмите кнопку  .
3. В появившемся окне выберите почтовый клиент для отправки файла.
   Автоматически будут заполнены строки "От", "Тема" и вложен файл CRL.
4. В окне почтового клиента впишите адрес получателя и отправьте письмо.

Для удаления CRL:

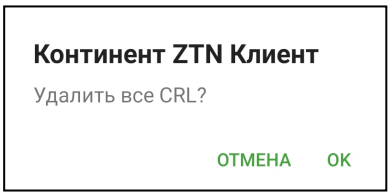
1. В окне "CRL" проведите пальцем справа налево по строке с CRL.
2. Нажмите кнопку  .
   На экране появится запрос на удаление CRL.



3. Нажмите кнопку "ОК".

Для удаления всех CRL:

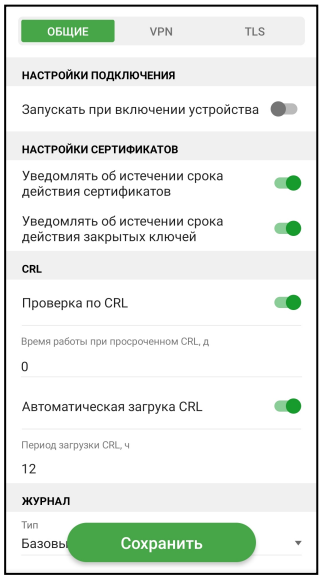
1. В меню окна "CRL" нажмите кнопку "Удалить все CRL".
   На экране появится запрос на удаление всех CRL.



2. Нажмите кнопку "ОК".

Окно "Настройки"

В окне выполняется настройка как общих параметров приложения, так и параметров подключения к СД в режимах работы VPN и TLS. Операции импорта и экспорта настроек также выполняются из меню окна настроек.



Для настройки параметров приложения:

1. В главном окне приложения вызовите меню и нажмите кнопку "Настройки". На экране появятся общие параметры приложения.
2. При необходимости выполните настройку следующих параметров:

Параметр	Описание
Вкладка "Общие"	
Запускать при включении устройства	Активируйте параметр, если необходимо запускать приложение при включении устройства. Значение по умолчанию — "ВЫКЛ"
Уведомлять об истечении срока действия сертификатов	Настройка получения уведомлений об истечении срока действия сертификатов и закрытых ключей. Значение по умолчанию — "ВКЛ"
Уведомлять об истечении срока действия закрытых ключей	
Проверка по CRL	Проверка актуальности сертификатов по списку отозванных сертификатов. Значение по умолчанию — "ВКЛ"
Время работы при просроченном CRL	Количество дней, по истечении которых невозможно установить соединение с СД, если список отозванных сертификатов устарел. Значение по умолчанию — 0
Автоматическая загрузка CRL	Автоматическое обновление списка отозванных сертификатов в период времени, установленный параметром "Период загрузки CRL". При отключенном параметре обновление CRL можно выполнить вручную в меню окна "CDP". Значение по умолчанию — "ВКЛ"
Период загрузки CRL	Периодичность обновления (в часах) списка отозванных сертификатов. Значение по умолчанию — 12
Тип	Уровень детализации журнала приложения. Значение по умолчанию — "Базовый"
Вкладка "VPN"	
Постоянное соединение	Соединение, отключаемое только средствами настройки параметров VPN-подключения, автоматически восстанавливается после потери сетевого соединения. Для активации предварительно настройте или активируйте профиль подключения. Значение по умолчанию — "ВЫКЛ". Недоступно для управления, если активирован параметр "Переподключение"
Переподключение	Автоматическое переподключение при потере сетевого соединения или при разрыве защищенного канала по инициативе сервера доступа АПКШ "Континент". Значение по умолчанию — "ВКЛ". Недоступно для управления, если активирован параметр "Переподключение"
Количество попыток переподключения	После последней неудачной попытки, количество которых задается пользователем, выводится сообщение об ошибке подключения. Значение по умолчанию — 3. Доступно для управления только при активации параметра "Переподключение"

Параметр	Описание
Время ожидания переподключения	Пауза (в секундах) между попытками подключения. Значение по умолчанию — 30. Доступно для управления только при активации параметра "Переподключение"
Время ожидания при бездействии	Время неактивности (в секундах), по истечении которого произойдет отключение от СД. Под неактивностью понимается отсутствие трафика в защищенном канале. Значение по умолчанию — 600. Доступно для управления только при активации параметра "Переподключение"
Вкладка "TLS"	
Сертификат по умолчанию	Импортируемый пользовательский сертификат приложения, необходимый для корректного подключения к защищенным ресурсам
Подтверждать сброс соединений	Активируйте параметр, если необходимо подтверждать сброс соединений. Значение по умолчанию — "ВКЛ"
Протокол TLS	Тип используемых TLS-протоколов. Значение по умолчанию — "TLS 1.0 и TLS 1.2"
Использовать шифронаборы	Активируйте параметр, если необходимо использовать шифронаборы. Значение по умолчанию — "ВЫКЛ"
Шифронабор "Магма"	Управление использованием шифронаборов "Магма" и "Кузнечик". Значение по умолчанию — "ВЫКЛ" Доступно для управления только при активации параметра "Использовать шифронаборы"
Шифронабор "Кузнечик"	
Автоматическое обновление	Автоматическое обновления списка ресурсов, загружаемых с сервера. При отключенном параметре обновление списка ресурсов можно выполнить вручную с помощью панели "Ресурсы". Значение по умолчанию — "ВКЛ"
Период обновления	Период обновления (в часах) списка ресурсов, загружаемых с сервера. Значение по умолчанию — 1. Доступно для управления только при активации параметра "Автоматическое обновление"

Импорт настроек

Примечание. Данная функция предназначена для переноса настроек с одного устройства на другое исключительно для конкретного пользователя. Не передавайте файл с настройками другим пользователям.

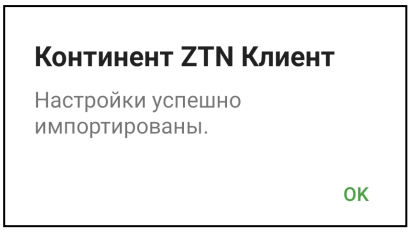
Операция предназначена для установки пакета настроек из приложения, установленного на другом устройстве. Перед выполнением импорта создайте папку и разместите в ней файл настроек "settings.json".

Для импорта настроек:

1. В главном окне приложения вызовите меню и нажмите кнопку "Настройки".
2. Вызовите меню в окне "Настройки" и нажмите кнопку "Импортировать настройки".

   Откроется директория внутренней памяти устройства.
3. Выберите в нужной папке файл настроек.

На экране появится сообщение об успешном импорте настроек.



4. Нажмите кнопку "ОК".

   Континент ZTN Клиент настроится автоматически и отобразит главное окно приложения.

Экспорт настроек

Примечание. Данная функция предназначена для переноса настроек с одного устройства на другое исключительно для конкретного пользователя. Не передавайте файл с настройками другим пользователям.

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

Для экспорта настроек:

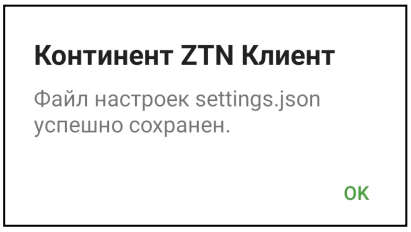
1. В главном окне приложения вызовите меню и нажмите кнопку "Настройки".
2. Вызовите меню в окне "Настройки" и нажмите кнопку "Экспортировать настройки".

   На экране появится запрос на сохранение файла настроек.

3. Нажмите кнопку "ОК".

   Приложение предложит выбрать папку для сохранения файла.
4. Выберите нужную папку.

   На экране появится сообщение об успешном сохранении файла.



5. Нажмите кнопку "ОК".

   Приложение вернет пользователя в окно "Настройки".

Любым доступным способом извлеките из памяти устройства сохраненный файл и передайте на другое устройство для выполнения операции импорта настроек.

Глава 4
Служебные операции

Обновление

Обновление приложения выполняется при переходе на новую версию в стандартном магазине приложений (например, в Google Play).

Примечание.
- В зависимости от настроек устройства пользователя приложения могут обновляться автоматически. Проверить версию приложения "Континент ZTN Клиент", установленную на устройстве, можно в окне "О программе".
- Для работы с Google Play необходимо наличие учетной записи Google.

Для обновления приложения вручную:

- В стандартном магазине приложений найдите приложение "Континент ZTN Клиент" и выполните стандартную процедуру обновления.

Контроль целостности

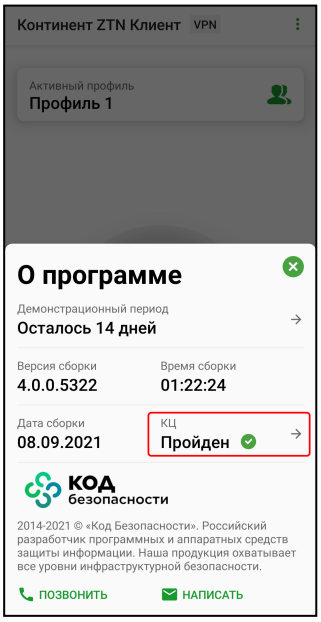
Контроль целостности файлов заключается в сравнении текущих значений контрольных сумм с эталонными значениями контрольных сумм динамических библиотек, заранее вычисленных при установке приложения на устройстве.

Контроль целостности приложения осуществляется:

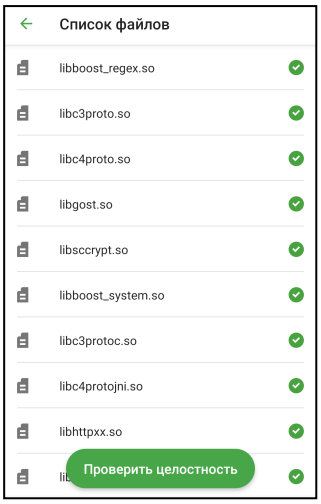
- при каждом запуске приложения;
- перед подключением к СД;
- перед созданием запроса на сертификат;
- после вызова информационного окна "О программе";
- пользователем вручную.

Для проведения КЦ:

1. В главном окне приложения вызовите меню и нажмите кнопку "О программе".
2. В появившемся окне нажмите на область, указанную на рисунке ниже.

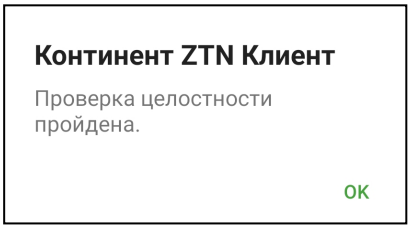


Откроется окно "Список файлов".



3. Нажмите кнопку "Проверить целостность".

   Если КЦ пройден успешно, появится соответствующее сообщение.



4. Нажмите кнопку "ОК".

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

Журнал

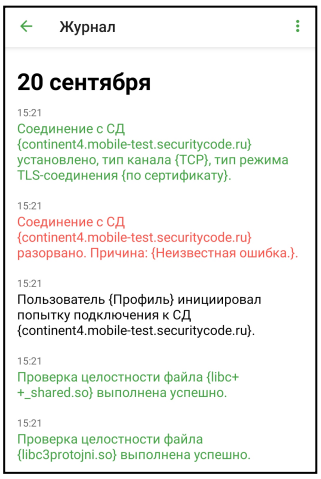
Журнал работы приложения

В окне "Журнал" содержатся сведения о работе приложения с момента его установки.

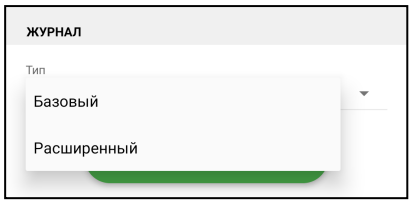
Для работы с журналом:

1. В главном окне приложения вызовите меню и нажмите кнопку "Журнал".

   Откроется журнал работы приложения.



В журнале предусмотрены два уровня детализации: базовый и расширенный. Настройка уровня детализации выполняется в окне "Настройки" (см. стр. **38**).



Возможные события, уровни их детализации и цветовые обозначения представлены в таблице ниже. Черный цвет используется для обычных событий, зеленый — для событий, связанных с успешным выполнением операций, красный — для событий, связанных с ошибками:

Уровень детализации	Цвет	Событие
Базовый	Черный	"Континент ZTN Клиент" запущен
Базовый	Черный	Добавлен профиль
Базовый	Черный	Удален профиль
Базовый	Черный	Сертификат пользователя добавлен в хранилище
Базовый	Черный	Сертификат пользователя удален
Базовый	Черный	Пользователь инициировал попытку подключения к СД
Базовый	Черный	Выполнен импорт файла с настройками
Базовый	Черный	Корневой сертификат добавлен в хранилище
Базовый	Черный	Корневой сертификат удален
Базовый	Черный	Импортирован CRL из файла
Базовый	Черный	Добавлен защищенный ресурс
Базовый	Черный	Удален защищенный ресурс
Базовый	Черный	Параметры проверки сертификатов изменены
Базовый	Черный	Добавлен CDP
Базовый	Черный	Отредактированы параметры CDP
Базовый	Зеленый	Соединение с СД установлено
Базовый	Зеленый	Установлено соединение с защищенным ресурсом
Базовый	Зеленый	Проверка целостности файла выполнена успешно
Базовый	Красный	Соединение с СД разорвано
Базовый	Красный	Произошла системная ошибка
Базовый	Красный	Не удалось проверить наличие обновлений списка ресурсов TLS-сервера
Базовый	Красный	Нарушена целостность файла. Создание новых сессий запрещено
Расширенный	Черный	Загрузка CRL
Расширенный	Черный	Выполнен перерасчет контрольной суммы файла
Расширенный	Черный	Параметры подключения к СД изменены
Расширенный	Черный	Автоматическое конфигурирование перечня ресурсов

Уровень детализации	Цвет	Событие
Расширенный	Зеленый	Континент ZTN Клиент успешно установлен
Расширенный	Зеленый	Создан запрос на сертификат
Расширенный	Зеленый	Инициализация процедуры проверки целостности файлов выполнена успешно
Расширенный	Зеленый	Самотестирование криптографических функций выполнено успешно
Расширенный	Красный	СД не ответил на отклик за указанное время
Расширенный	Красный	СД разорвал соединение
Расширенный	Красный	Ошибка подключения: использован неподдерживаемый на СД режим организации VPN-соединения
Расширенный	Красный	Ошибка ввода пароля для доступа к ключевому контейнеру для сертификата
Расширенный	Красный	Ошибка подключения: истек срок действия закрытого ключа для сертификата
Расширенный	Красный	Ошибка инициализации процедуры проверки целостности файлов. Требуется переустановка приложения
Расширенный	Красный	Истек срок действия закрытого ключа сертификата
Расширенный	Красный	Сервер разорвал соединение на этапе аутентификации
Расширенный	Красный	Выполнен сброс всех соединений
Расширенный	Красный	Работа приложения завершена с ошибкой

Для отправки журнала:

1. В окне "Журнал" вызовите меню и нажмите кнопку "Отправить журнал".

   На экране появится запрос на сохранение журнала.
2. Нажмите кнопку "ОК".

   Откроется директория внутренней памяти устройства.
3. Выберите папку для сохранения файла журнала.

   Файл журнала будет создан и сохранен в указанную папку.
4. Нажмите кнопку "ОК".
5. В появившемся окне выберите почтовый клиент для отправки журнала.

   В окне почтового клиента автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.
6. Впишите адрес и отправьте письмо администратору.

Отладочный журнал

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

Для отправки журнала:

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

   Будет выполнено сохранение отладочной информации.

   Примечание. Файл отладочного журнала по умолчанию сохраняется по следующему пути: /Память устройства/Android/data/ru.securitycode.continentapp/files/logcat.log.
2. В появившемся окне выберите почтовый клиент для отправки журнала.

В окне почтового клиента автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.

3. Впишите адрес и отправьте письмо администратору.

Управление режимом работы

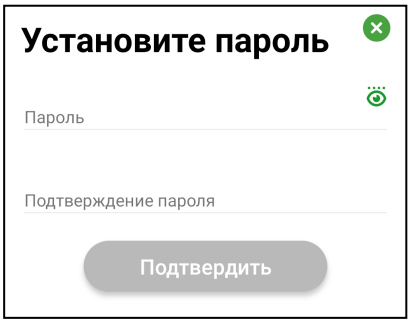
Континент ZTN Клиент функционирует в двух режимах:

Основной режим
Установлен по умолчанию. Пользователю предоставляются права полного доступа. Права в основном режиме: • подключение/отключение к/от СД в режиме работы VPN; • установление и разрыв соединений с защищенными ресурсами в режиме работы TLS; • просмотр списка профилей; • создание и удаление профиля; • просмотр информации о профиле и его настройка; • просмотр списка серверов /ресурсов; • просмотр и обновление ресурсов, загруженных с сервера; • добавление и удаление серверов /ресурсов; • настройка серверов /ресурсов; • импорт конфигурации; • экспорт/импорт настроек; • создание запроса на сертификат; • импорт сертификатов и ключа; • просмотр импортированных сертификатов; • просмотр сведений о сертификате; • скрытие сертификатов и ключа во внутренней памяти устройства; • удаление сертификатов и ключа; • управление CDP и CRL; • просмотр и редактирование настроек подключения; • смена режима работы; • просмотр журнала; • просмотр окна "О программе"; • контроль целостности
Режим ограниченной функциональности
Пользователю предоставляются права ограниченного доступа к управлению настройками приложения. Права в режиме ограниченной функциональности: • подключение/отключение к/от СД в режиме работы VPN; • установление и разрыв соединений с защищенными ресурсами в режиме работы TLS; • просмотр журнала; • просмотр окна "О программе"; • контроль целостности

Для смены режима работы:

1. В главном окне приложения вызовите меню и нажмите кнопку "Сменить режим работы".

   На экране появится окно установки пароля.



2. Установите пароль блокировки, указав его в полях "Пароль" и "Подтверждение пароля".
3. Нажмите кнопку "Подтвердить".

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

Чтобы сменить режим работы, выполните предыдущую операцию еще раз. Если надпись "Режим ограниченной функциональности" в главном окне приложения пропала, активирован основной режим.