КОД безопасности

Средство криптографической защиты информации

Континент ZTN Клиент для Android

Руководство пользователя

АМБС.26.20.40.140.005 92

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 пользователей изделия "Средство криптографической защиты информации "Континент ZTN Клиент для Android" АМБС.26.20.40.140.005 (далее — Континент ZTN Клиент, приложение). В нем содержатся сведения, необходимые пользователю для доступа к защищаемым ресурсам средствами приложения "Континент ZTN Клиент" на платформе Android.

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

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.

Установка и подключение приложения

Установка и первый запуск приложения

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

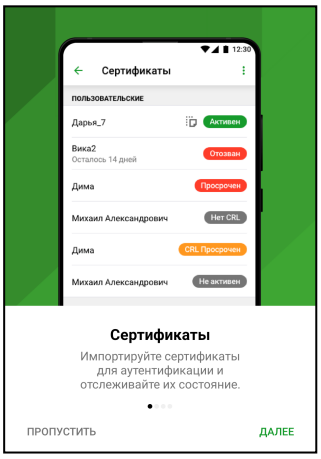
Внимание!

- 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.

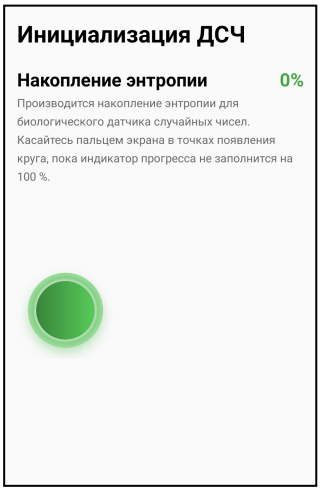
   При первом запуске появятся обучающие экраны.



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.

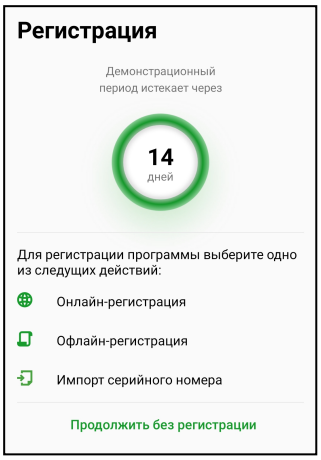
На экране появится сообщение с инструкцией и индикатором накопления энтропии для биологического датчика случайных чисел.



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.

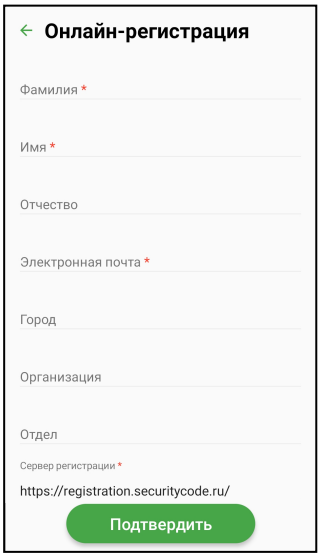
Если по истечении срока демонстрационного периода приложение не зарегистрировано, при каждом запуске будет открываться экран регистрации с соответствующим сообщением. Пропустить регистрацию по истечении этого срока будет невозможно. Экран регистрации также можно вызвать в окне "О программе", нажав на 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. **6**) 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".

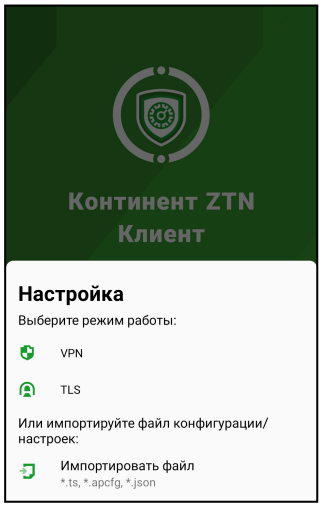
   На экране появится директория внутренней памяти устройства.

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 или настроек.

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. **11**) и передает его администратору.
   - Администратор выпускает корневой и пользовательский сертификаты и передает их пользователю.
   - Пользователь импортирует сертификаты на экране предварительной настройки приложения (см. стр. **7**) и выполняет настройку параметров профиля (см. стр. **16**).

   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. **16**).

Импорт файла с экрана предварительной настройки приложения

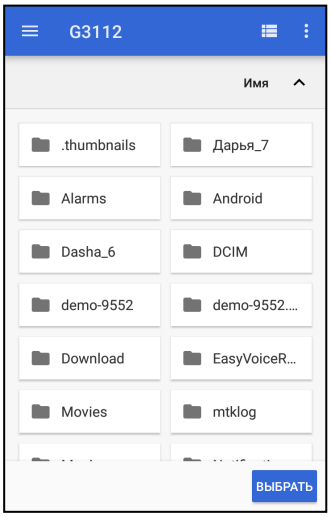
В случае установки конфигурации файл скачивается в формате "XXX.ts4" или "XXX.apcfg" (в зависимости от версии сервера доступа), в случае установки настроек — в формате "settings.json". Перед выполнением операции импорта создайте папку и разместите в ней скачанный файл.

Примечание. Функция "Импортировать файл" предназначена для переноса настроек с одного устройства на другое только для конкретного пользователя. Не передавайте файл другим пользователям.

Для импорта файла:

1. В окне предварительной настройки приложения (см. стр. **7**) нажмите кнопку "Импортировать файл".

   На экране появится директория внутренней памяти устройства.



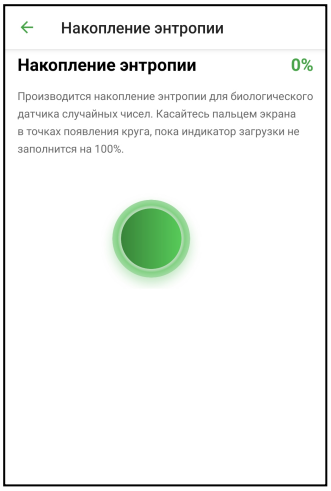
2. Откройте на устройстве папку, в которой содержится файл, а затем выберите его.

При импорте файла настроек приложение настроится автоматически. На экране появится сообщение об успешно выполненной операции, и откроется главное окно приложения (см. стр. **10**).

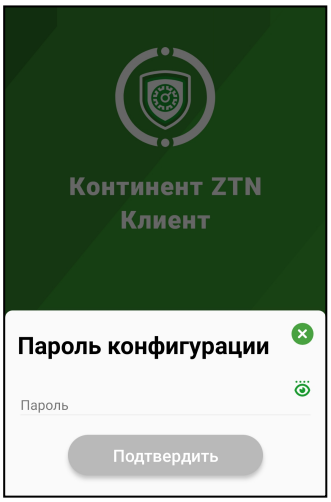
При импорте файла конфигурации в зависимости от состава файла пользователь выполняет следующие операции в различных сочетаниях:

Примечание. Учетные данные для завершения операции импорта конфигурации выдает администратор.

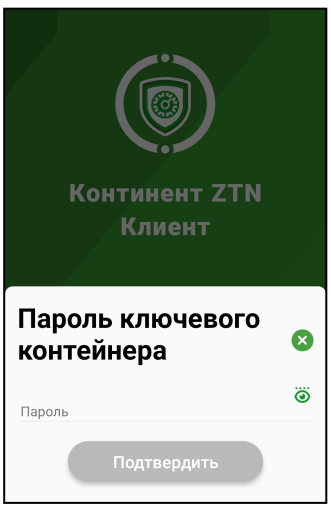
- накопление энтропии;



- ввод пароля для файла конфигурации;



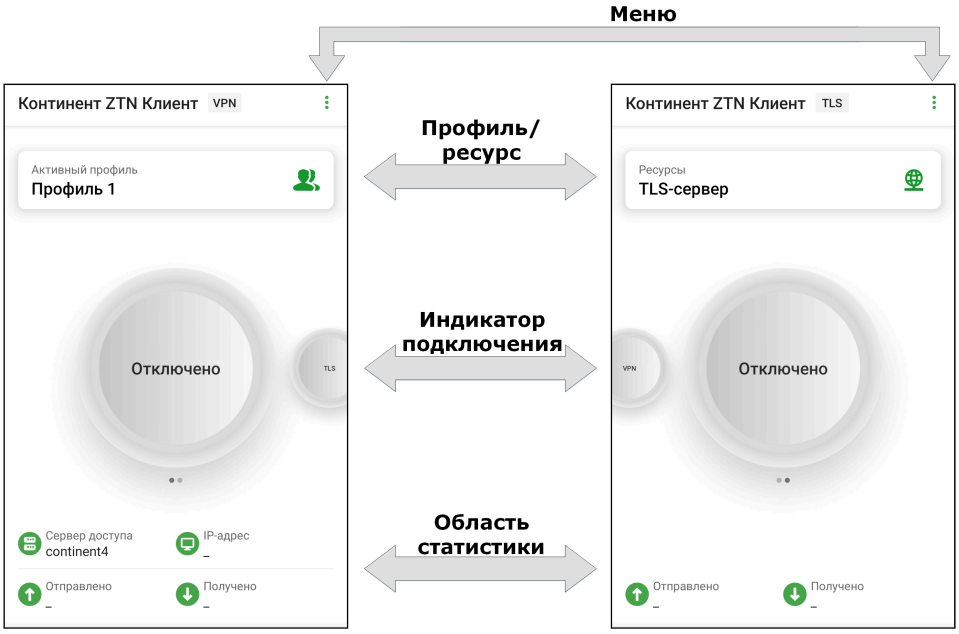
- ввод пароля для ключевого контейнера.



По окончании импорта на экране появится сообщение об успешном выполнении операции.

3. Нажмите кнопку "ОК".

   Откроется главное окно приложения.



Импорт файла из меню приложения

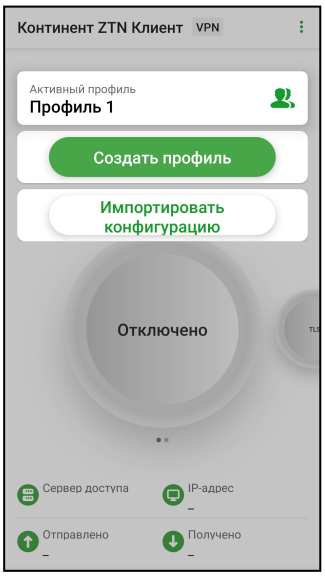
Операция предназначена для установки пакета настроек на уже установленном и настроенном приложении. Перед выполнением импорта создайте папку. В случае импорта настроек разместите в ней файл "settings.json", в случае импорта конфигурации — файл "XXX.ts4" или "XXX.apcfg" (в зависимости от версии сервера доступа).

Примечание. Функция "Импортировать файл" предназначена для переноса настроек с одного устройства на другое только для конкретного пользователя. Не передавайте файл другим пользователям.

Для импорта файла конфигурации:

1. В главном окне на странице "VPN" выберите панель "Активный профиль".

   Окно примет вид, подобный следующему.



2. Нажмите кнопку "Импортировать конфигурацию".

   Откроется директория внутренней памяти устройства.

3. Выберите в нужной папке файл конфигурации.

   При импорте конфигурации в зависимости от состава файла пользователь выполняет следующие операции в различных сочетаниях:

   Примечание. Учетные данные для завершения импорта конфигурации выдает администратор.

   - накопление энтропии (см. стр. 9);
   - ввод пароля для файла конфигурации (см. стр. 9);
   - ввод пароля для ключевого контейнера (см. стр. 9).

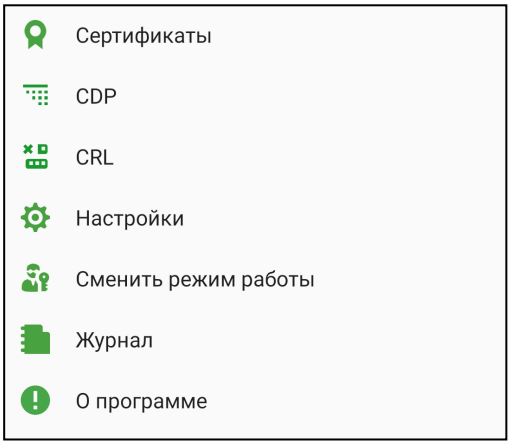
   По окончании импорта на экране появится сообщение об успешном выполнении операции.

4. Нажмите кнопку "ОК".

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

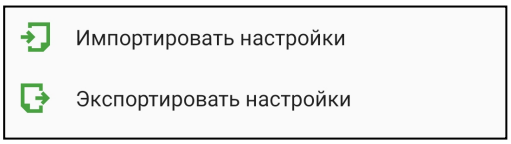
Для импорта файла настроек:

1. В главном окне приложения вызовите меню.



2. Нажмите кнопку "Настройки" и вызовите меню в открывшемся окне.

   Меню появится в нижней части экрана.



3. Нажмите кнопку "Импортировать настройки".

   Откроется директория внутренней памяти устройства.

4. Выберите в нужной папке файл настроек.

   По окончании импорта на экране появится сообщение об успешном выполнении операции.

5. Нажмите кнопку "ОК".

   Континент ZTN Клиент настроится автоматически, и на экране появится главное окно приложения.

Ручная настройка приложения

Если файлы настроек и конфигурации отсутствуют, выполните ручную настройку приложения. Приложение имеет два режима работы — VPN и TLS.

Настройка приложения в режиме работы VPN

В приложении реализованы два способа получения сертификатов:

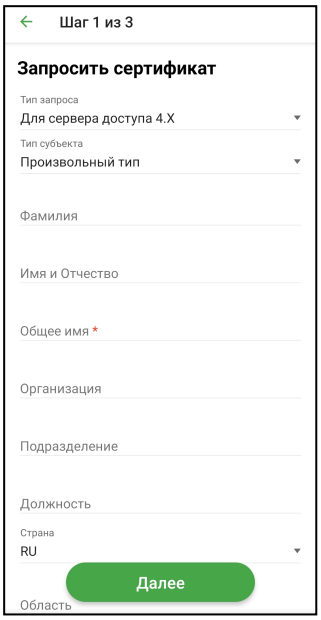
- загрузка файлов на мобильное устройство;
- оформление запроса на получение сертификата.

Шаг 1. Запрос на сертификат

Внимание! Перед созданием запроса получите у администратора безопасности сведения об используемом сервере доступа.

Для создания запроса на сертификат:

1. В окне предварительной настройки приложения нажмите кнопку "Запросить сертификат".



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

2. Введите сведения о пользователе.

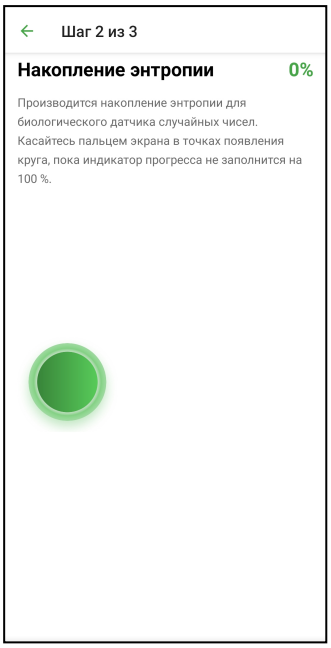
Примечание. Тип запроса зависит от версии сервера доступа.

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".

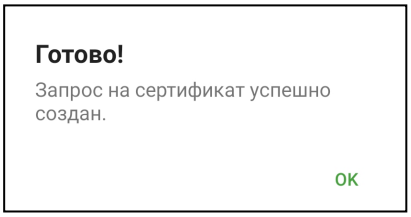
   На экране появится запрос на сохранение файла.

8. Нажмите кнопку "ОК".

   На экране появится директория внутренней памяти устройства.

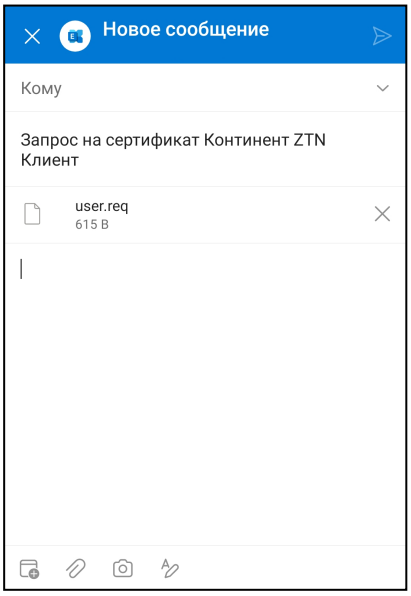
9. Выберите папку для сохранения запроса на сертификат и нажмите кнопку "Выбрать".

   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.

Примечание. В данном примере рассматривается почтовый клиент Microsoft Outlook.



В окне почтового клиента автоматически будет добавлен файл запроса и заполнено поле "Тема".

12. Заполните поле "Кому" и отправьте письмо администратору.

Шаг 2. Загрузка сертификата и ключевого контейнера на мобильное устройство

Администратор передает один из наборов файлов:

- полный набор — пользовательский и корневой сертификаты ("root.p7b" и "user.cer");
- самоподписанный корневой сертификат ("root.p7b").

Существуют два варианта загрузки файлов:

- Передача файлов сертификатов на мобильное устройство по электронной почте после запроса на получение сертификата.
- Передача файлов сертификатов на мобильное устройство при подключении к компьютеру. Скопируйте файлы сертификатов в папку, содержащую сертификаты, и отключите устройство от компьютера средствами безопасного отключения ОС.

Шаг 3. Импорт сертификата и настройка профиля

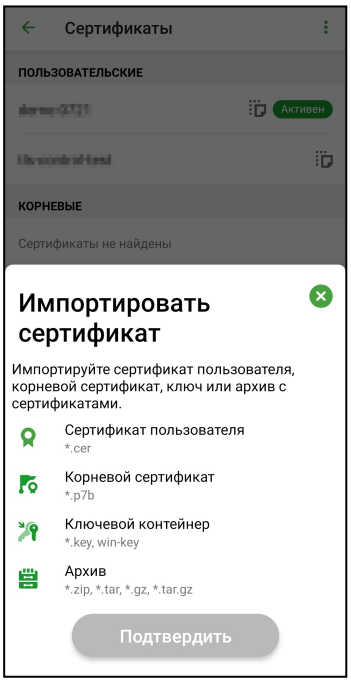
Внимание! Пользователь получает у администратора инструкции для настройки профиля и файлы сертификатов.

Для импорта сертификата:

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

1. В окне предварительной настройки приложения (см. стр. **7**) выберите режим работы VPN.
2. В открывшемся окне нажмите кнопку "Импортировать сертификат".

   На экране появится окно импорта сертификатов и ключа.

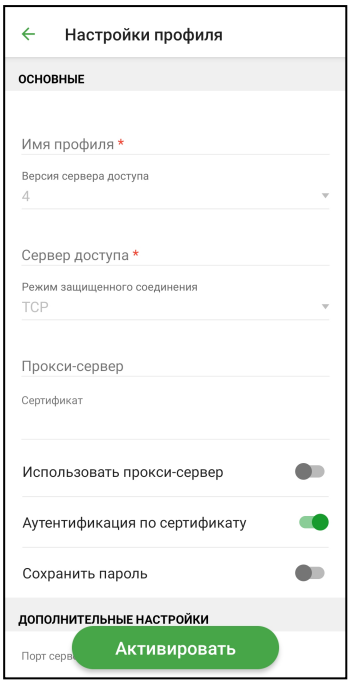


3. Выберите нужный тип импортируемого файла.

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

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

На экране появится окно "Настройки профиля".



6. Заполните доступные поля и нажмите кнопку "Активировать".

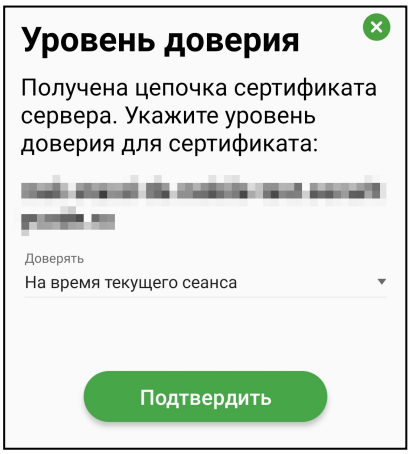
Настройка приложения в режиме работы TLS

Для добавления сервера/ресурса:

1. В окне предварительной настройки приложения (см. стр. 7) выберите режим работы TLS.
2. В открывшемся окне выберите тип соединения — сервер или ресурс.

   На экране появится окно добавления сервера/ресурса.
3. Заполните все поля и нажмите кнопку "Добавить".

   При добавлении сервера появится запрос с указанием уровня доверия.



4. Выберите из раскрывающегося списка уровень доверия для сертификата.
5. Нажмите кнопку "Подтвердить".

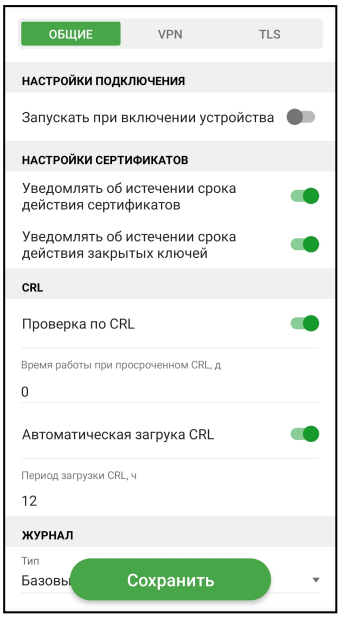
Настройка подключения

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

Для настройки параметров подключения:

1. Вызовите меню главного окна приложения 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 и нажмите кнопку "Сохранить".

Подключение к серверу доступа

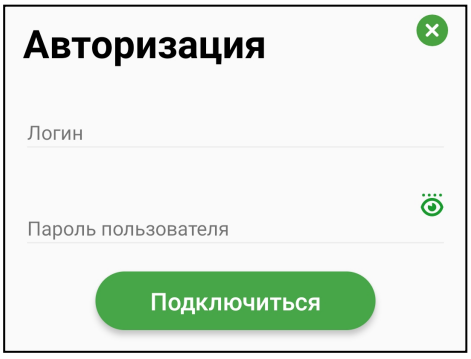
Для подключения к серверу доступа:

Примечание. Перед подключением к серверу доступа:
- на мобильном устройстве установите сертификат пользователя, корневой сертификат, а также ключевой контейнер;
- настройте профиль подключения к серверу доступа;
- настройте параметры подключения в режиме VPN.

1. В главном окне приложения (см. стр. **10**) 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.



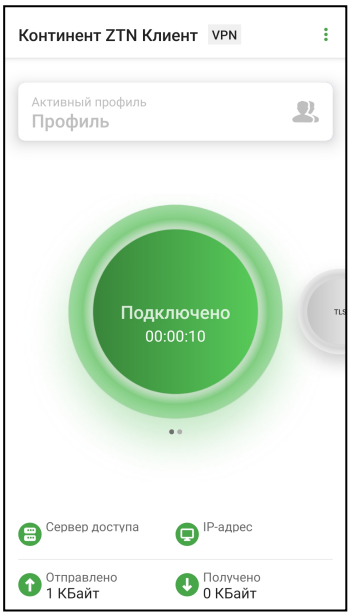
4. Введите логин и пароль, а затем нажмите кнопку "Подключиться".

   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 пользователю 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. **10**) 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.

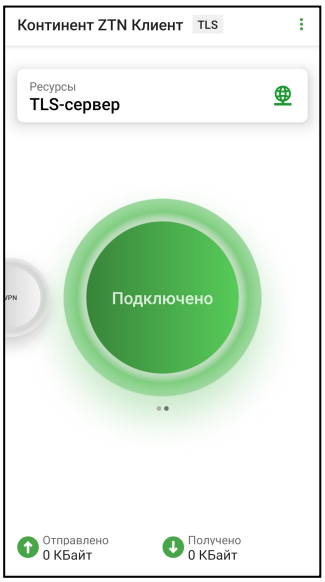
   На экране появится директория внутренней памяти устройства.

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.