КОД безопасности

# Континент ZTN Клиент для iOS, iPadOS

## Руководство по эксплуатации

АМБС.26.20.40.140.006 91



| | |
|---|---|
| Почтовый адрес: | **115127, Россия, Москва, а/я 66**<br>**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 |
| 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 |
| UUID | Universally Unique Identifier |
| VPN | Virtual Private Network |
| ZTN | Zero Trust Networking |

# Введение

Данное руководство предназначено для администраторов и пользователей изделия "Континент ZTN Клиент для iOS, iPadOS" АМБС.26.20.40.140.006 (далее — Континент ZTN Клиент, Клиент, приложение). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации Клиента.

**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

Приложение "Континент ZTN Клиент" устанавливается на мобильные устройства, функционирующие под управлением операционных систем iOS, iPadOS версий 14–16.

Континент ZTN Клиент реализует следующие основные функции:

- установление защищенного соединения и обмен зашифрованными данными с сервером доступа изделия "Аппаратно-программный комплекс шифрования "Континент" версии 3.9 (далее — АПКШ "Континент") и узлом безопасности с включенным компонентом "Сервер доступа" изделия "Комплекс безопасности "Континент". Версия 4" (далее — комплекс "Континент");
- установление защищенного соединения с изделием "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее — TLS-сервер), а также обмен данными с веб-серверами корпоративной сети;
- контроль целостности файлов программного обеспечения;
- регистрация событий, связанных с функционированием приложения.

Континент ZTN Клиент поддерживает работу по протоколу TLS версий 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 технические характеристики, приведенные в таблице ниже.

| **Алгоритм шифрования** |
|---|
| В соответствии с ГОСТ Р 34.12-2015 в режиме гаммирования согласно ГОСТ Р 34.13-2015 |
| **Защита передаваемых данных от искажения** |
| В соответствии с ГОСТ Р 34.12-2015 в режиме гаммирования согласно ГОСТ Р 34.13-2015 |
| **Расчет хэш-функции** |
| В соответствии с ГОСТ Р 34.11-2012 |
| **Формирование и проверка электронной подписи** |
| В соответствии с ГОСТ Р 34.10-2012 |

## Принципы функционирования

### Режим VPN

Континент ZTN Клиент в режиме VPN позволяет осуществлять установление защищенного соединения и обмен зашифрованными данными с сервером доступа АПКШ "Континент" и узлом безопасности с включенным компонентом "Сервер доступа" комплекса "Континент" через общедоступные (незащищенные) сети.

Континент ZTN Клиент поддерживает соединение по протоколу версии 4. Для соединения используется протокол TCP, а аутентификация осуществляется с помощью сертификата пользователя и ключевого контейнера или логина и пароля.

### Режим TLS

Континент ZTN Клиент в режиме TLS предназначен для реализации защищенного доступа удаленных пользователей к веб-ресурсам корпоративной сети по каналам связи общих сетей передачи данных с использованием алгоритмов, соответствующих ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015.

Для подключения к защищаемым веб-ресурсам корпоративной сети удаленный пользователь должен выбрать веб-ресурс из списка в приложении или ввести имя веб-ресурса в адресной строке веб-браузера. По указанному имени 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 приложением и TLS-сервером устанавливается защищенное соединение по протоколу TLS. Далее TLS-сервер направляет запрос приложению по указанному пользователем адресу веб-ресурса в защищаемую сеть. Полученный от веб-сервера ответ на запрос TLS-сервер возвращает в рамках защищенного соединения.

При невыполнении по каким-либо причинам требований, предъявляемых к аутентификации приложения и TLS- сервера, защищенное соединение не устанавливается и доступ пользователя к веб- ресурсу блокируется.

## Сертификаты

Для создания защищенного соединения между устройством и СД пользователь получает у администратора безопасности и устанавливает на мобильном устройстве сертификат пользователя, корневой сертификат, удостоверяющий сертификат пользователя, а также — корневой сертификат, удостоверяющий сертификат сервера.

Пользователь может получить сертификаты одним из следующих способов:

- Администратор передает пользователю корневой и пользовательский сертификаты вместе с закрытым ключом пользователя, записанным на карте памяти или внешнем носителе.
- Пользователь создает в приложении запрос на получение сертификата. Пользователь передает администратору созданный запрос, на основании которого администратор создает сертификат и передает его пользователю вместе с корневым сертификатом.

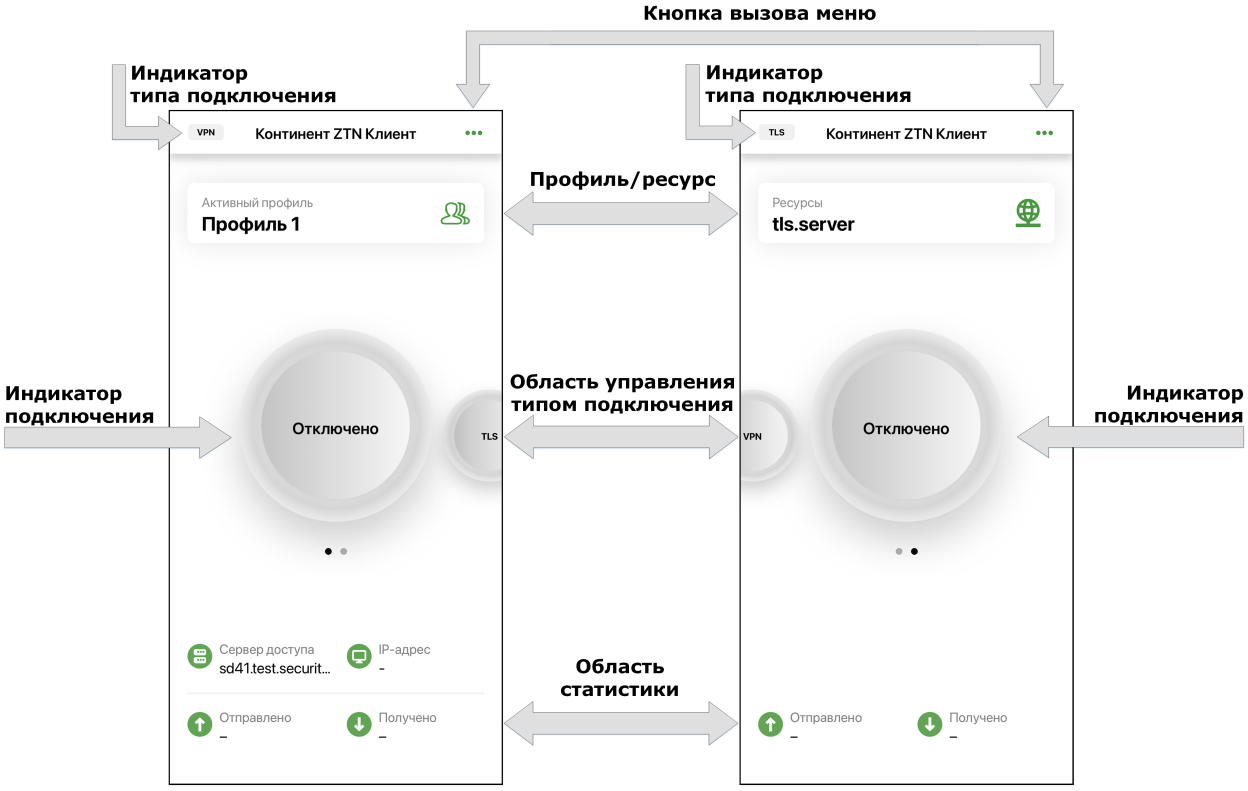
**Примечание.** Передача файлов сертификатов должна выполняться по защищенным каналам связи.

Поддерживается работа с ключами форматов PKCS#15 и 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 формирования закрытого ключа. По истечении этого срока работа с сертификатом будет невозможна. Необходимо осуществить перевыпуск сертификата пользователя с закрытым ключом.

## Пользовательский интерфейс главного окна

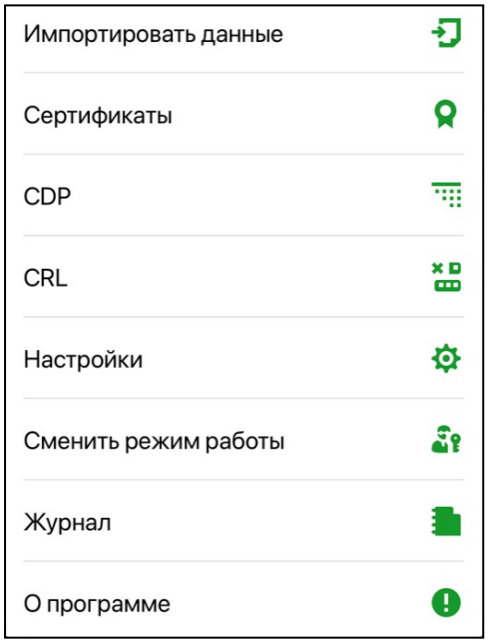
Для управления Клиентом реализовано специализированное ПО с графическим пользовательским интерфейсом, устанавливаемое на мобильные устройства.



Главное окно состоит из объектов, приведенных ниже.

| Объект | Описание |
|---|---|
| **Индикатор типа подключения** | Наименование страницы главного экрана приложения — VPN или TLS |
| **Меню** | Разделы для импорта данных, работы с сертификатами, CDP и CRL, настройками приложения, смены режима работы, просмотра журналов и сведений о программе |
| **Активный профиль (VPN)** | Просмотр, создание, настройка и удаление профилей подключения для СД |
| **Ресурсы (TLS)** | Просмотр, добавление, настройка и удаление серверов/ресурсов |
| **Индикатор подключения** | В неактивном состоянии имеет серый цвет и надпись "Отключено". После установления подключения меняет цвет на зеленый, появляется надпись "Подключено".<br>При нажатии на индикатор подключения, в зависимости от страницы, осуществляется:<br>• подключение/отключение к/от СД в режиме работы VPN;<br>• активация режима работы TLS |
| **Область управления типом подключения** | В зависимости от страницы, в правой/левой части главного окна приложения отображается индикатор другого типа подключения.<br>При необходимости выполнить переключение:<br>• на страницу TLS — проведите пальцем вправо;<br>• на страницу VPN — проведите пальцем влево |
| **Область статистики** | Просмотр статистики текущей сессии |

Меню главного окна содержит разделы, приведенные ниже.




| Пункт меню | Описание |
|---|---|
| **Импортировать данные** | Импорт сертификатов (см. стр. **28**), конфигурации (см. стр. **21**) или настроек (см. стр. **35**) |
| **Сертификаты** | Просмотр сведений об импортированных сертификатах, импорт, удаление и скрытие во внутренней памяти устройства сертификатов и ключевых контейнеров (см. стр. **24**) |
| **CDP** | Просмотр, добавление, редактирование, удаление CDP и загрузка CRL (см. стр. **29**) |
| **CRL** | Просмотр и редактирование списка CRL, а также импорт CRL (см. стр. **31**) |
| **Настройки** | Просмотр и настройка общих параметров приложения, а также параметров режимов VPN и TLS (см. стр. **33**) |
| **Сменить режим работы** | Переключение режима работы приложения (см. стр. **35**) |
| **Журнал** | Просмотр сведений о работе приложения (см. стр. **37**) |
| **О программе** | Просмотр сведений о текущей версии ПО (см. стр. **39**) и статусе контроля целостности по результатам проверки контрольных сумм динамических библиотек (см. стр. **40**) |

# Глава 2
# Ввод в эксплуатацию

## Установка и первый запуск приложения

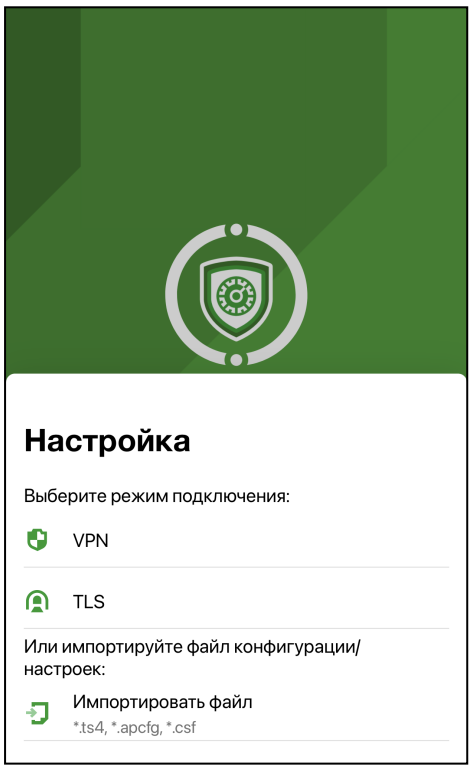
Установка приложения выполняется пользователем из магазина приложений App Store.

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

**Для установки и первого запуска:**

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

   На экране появится окно предварительной настройки приложения.




## Импорт файла для настройки приложения в режиме VPN

При импорте конфигурации используется файл с расширением "*.apcfg" или "*.ts4" для СД версий 3.X или 4.X соответственно, а при импорте настроек — файл с расширением "*.csf". После получения файла конфигурации/настроек создайте папку в каталоге Клиента и разместите в ней файл.

**Внимание!** Импорт конфигурации с использованием файла "XXX.apcfg" поддерживается только для подключения к СД по протоколу версии 4, а при импорте настроек профили, осуществляющие подключение по протоколу 3.X, импортированы не будут.

**Для импорта файла конфигурации:**

1. На экране предварительной настройки приложения (см. выше) нажмите кнопку "Импортировать файл".

   На экране появится директория внутренней памяти устройства.
2. Выберите файл конфигурации, содержащийся в созданной ранее папке, нажав кнопку "Выбрать".

   На экране появится окно ввода пароля доступа к конфигурации.
3. Введите пароль к файлу конфигурации и нажмите кнопку "Подтвердить".

   **Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к файлу конфигурации или ключевому контейнеру — 5. После 5 неудачных попыток импорт конфигурации будет автоматически отменен.

4. При необходимости в появившемся окне введите пароль доступа к ключевому контейнеру и нажмите кнопку "Подтвердить".

**Примечание.** В состав файла конфигурации может входить несколько ключевых контейнеров, профилей и т. д. Будет осуществлен импорт только первых в списке профиля, ключевого контейнера и т. д., остальные файлы будут проигнорированы.

На экране появится сообщение об успешном импорте файла.

5. Нажмите кнопку "ОК".

На экране появится главное окно приложения (см. стр. **7**).

**Для импорта файла настроек:**

1. На экране предварительной настройки приложения нажмите кнопку "Импортировать файл".

На экране появится директория внутренней памяти устройства.

2. Укажите требуемый файл настроек и нажмите кнопку "Выбрать".

На экране появится сообщение об успешном импорте настроек.

3. Нажмите кнопку "ОК".

На экране появится главное окно приложения.

# Ручная настройка приложения в режиме VPN

Ручная настройка выполняется с помощью файлов сертификатов, если отсутствует файл конфигурации/настроек. По требованию администратора пользователь создает на мобильном устройстве запрос на сертификат пользователя.

Администратор передает файлы сертификатов одним из следующих способов:

- пользовательский и корневой сертификаты ("user.cer" и "root.p7b");
- корневой сертификат ("root.p7b").

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

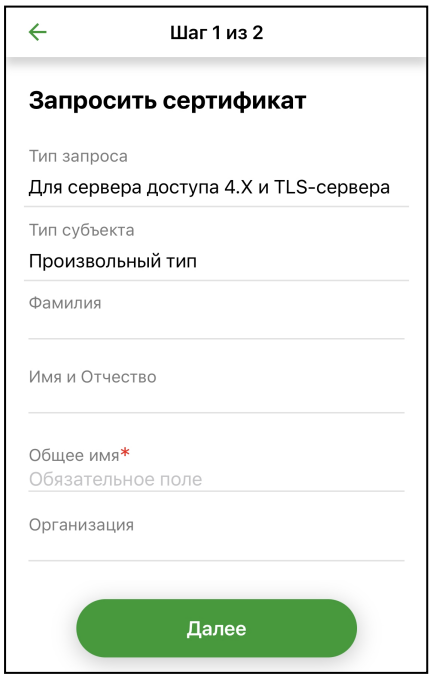
Перед выполнением импорта создайте папку в каталоге Клиента и разместите в ней полученные файлы.

## Создание запроса на сертификат

**Для создания запроса на сертификат:**

1. На экране предварительной настройки (см. стр. **9**) нажмите кнопку "VPN".
2. В появившемся окне нажмите кнопку "Запросить сертификат".

На экране появится окно создания запроса на получение сертификата.



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

3. Укажите сведения о пользователе.

**Примечание.** Тип запроса зависит от версии СД сервера доступа. Выпуск сертификатов по запросам типа "Для сервера доступа 3.X" должен осуществляться средствами СД соответствующих версий. В противном случае импорт таких сертификатов может завершиться ошибкой.

В зависимости от выбранного типа субъекта обязательными являются поля, указанные ниже.

| 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 ФЛ** | | + | + | | + |
| **ИНН ЮЛ** | | | | | |
| **СНИЛС** | | + | | + | |
| **ОГРН** | | | + | | + |
| **ОГРНИП** | | | | + | |

4. Нажмите кнопку "Далее".

   На экране появится окно установки пароля доступа к ключевому контейнеру.

5. Введите пароль и подтвердите его в требуемых полях.

**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".

**Примечание.**
- При нажатии кнопки "Сохранить" выполните пп. **8, 9**. После этого передайте файл запроса администратору.
- Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи.

   На экране появится директория внутренней памяти устройства.

8. Укажите папку для сохранения файла запроса и нажмите кнопку "Выбрать" либо создайте новую, нажав кнопку "Создать папку".

9. В появившемся окне нажмите кнопку "ОК".

   На экране появится окно выбора способа отправки файла.

10. Выберите требуемый почтовый клиент.

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

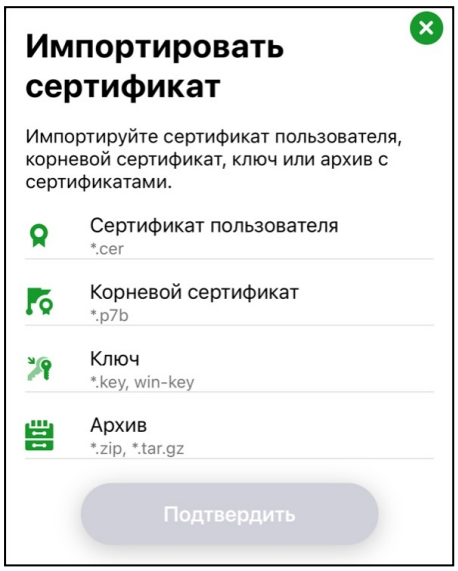
11. Впишите адрес и отправьте письмо администратору.

12. После получения файлов сертификатов выполните их импорт (см. стр. **12**).

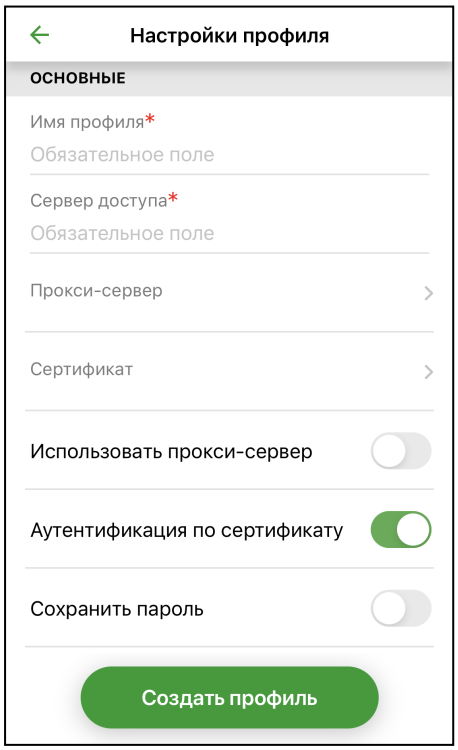
## Импорт сертификатов

**Для импорта сертификатов:**

1. На экране предварительной настройки приложения (см. стр. 9) нажмите кнопку "VPN".
2. В появившемся окне нажмите кнопку "Запросить сертификат".
   На экране появится окно импорта сертификатов и ключа.




3. Выберите требуемый пункт.
   На экране появится директория внутренней памяти устройства.
4. Выберите файл сертификата или архив, содержащий файлы сертификатов.
5. При необходимости повторите действия, описанные в пп. **2**, **3**.
6. Нажмите кнопку "Подтвердить".
   На экране появится сообщение об успешном импорте.
7. Нажмите кнопку "ОК".
   На экране появится окно создания профиля.



## Создание профиля

**Для создания профиля:**

1. В окне создания профиля укажите значения для параметров настроек профиля, приведенных ниже.

| |
|---|
| **Имя профиля** |
| Наименование профиля для подключения к СД |
| **Сервер доступа** |
| IP-адрес или DNS-имя сервера доступа |
| **Прокси-сервер** |
| При нажатии на строку открывается окно настройки прокси-сервера со следующими параметрами:<br>• адрес — IP-адрес или имя прокси-сервера;<br>• порт — порт прокси-сервера. Значение по умолчанию — 3128;<br>• аутентификация — тип аутентификации на прокси-сервере. Значение по умолчанию — "Без аутентификации" |
| **Сертификат** |
| Сертификат, используемый для подключения. При нажатии на строку параметра необходимо выбрать сертификат в раскрывающемся списке, содержащем импортированный ранее пользовательский сертификат.<br>Доступно для настройки только при активированном параметре "Аутентификация по сертификату" |
| **Использовать прокси-сервер** |
| Значение по умолчанию — "ВЫКЛ". Доступно для активации после настройки параметров в окне "Прокси-сервер" |
| **Аутентификация по сертификату** |
| Аутентификация осуществляется по пользовательскому сертификату, указанному в поле "Сертификат". При деактивации параметра аутентификация осуществляется по логину и паролю. Значение по умолчанию — "ВКЛ". |
| **Сохранить пароль** |
| Отвечает за сохранение пароля при повторном подключении к СД. Значение по умолчанию — "ВЫКЛ". При активации параметра после ввода пароля он будет сохранен, окно запроса пароля больше появляться не будет |
| **Дополнительные настройки** |
| Доступны следующие дополнительные параметры для настройки профиля:<br>• порт сервера доступа (значение по умолчанию — 443);<br>• порт клиента — порт мобильного устройства. Значение по умолчанию — 7500;<br>• основной DNS-сервер, альтернативный DNS-сервер — по умолчанию используются адреса DNS-серверов, получаемые от СД. Если адреса не получены, их необходимо указать вручную. Адреса, полученные от СД, имеют приоритет над адресами, указанными вручную;<br>• домен — при необходимости можно указать DNS-суффикс, автоматически добавляемый к имени хоста при обращении к защищенным ресурсам;<br>• MTU — максимальный размер блока (в байтах) на канальном уровне сети. Значение по умолчанию — 1500 |

2. Нажмите кнопку "Активировать".
3. В появившемся окне нажмите кнопку "ОК".

   На экране появится главное окно приложения (см. стр. 7).

## Подключение к серверу доступа

**Для подключения к серверу доступа:**

**Примечание.** Для сертификатов, выпущенных на СД, CRL не требуется. Для подключения к СД отключите проверку по CRL и, при необходимости, выполните настройку других параметров приложения.

1. В главном окне приложения (см. стр. 7) перейдите на страницу "VPN".
2. Выберите панель "Активный профиль" и активируйте в списке требуемый профиль.
3. Нажмите на индикатор подключения.

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

**Примечание.** В данном примере рассматривается вариант ввода пароля доступа к ключевому контейнеру.

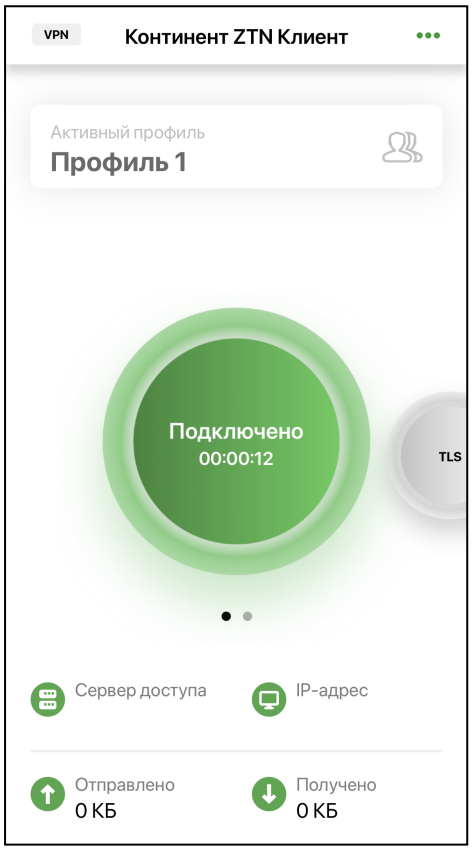
4. Введите пароль доступа к ключевому контейнеру и нажмите кнопку "Подтвердить".

**Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к ключевому контейнеру — 5.

Если в настройках профиля переключатель "Сохранить пароль" деактивирован, на экране появится окно с предложением сохранить пароль.

5. Выполните одно из следующих действий:
   - нажмите кнопку "Да" — пароль будет сохранен, при следующих подключениях по текущему профилю окно ввода пароля появляться не будет;
   - нажмите кнопку "Нет" — окно закроется, при следующем подключении по текущему профилю окно ввода пароля появится снова;
   - нажмите кнопку "Никогда для этого профиля" — окно закроется и больше появляться не будет, для текущего профиля при следующих подключениях будет появляться только окно ввода пароля.

Если пароль доступа введен корректно, индикатор подключения изменит цвет на зеленый.




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

**Примечание.** Раз в полгода пользователю необходимо менять пароль ключевого контейнера. Перед подключением к СД осуществляется проверка срока действия пароля к контейнеру. По окончании срока действия пароля к контейнеру на экране появится окно, где пользователь должен ввести и подтвердить новый пароль.

## Импорт файла для настройки приложения в режиме TLS

При импорте настроек используется файл с расширением "*.csf". После получения файла настроек создайте папку в каталоге Клиента и разместите в ней файл.

**Для импорта файла настроек:**

1. На экране предварительной настройки приложения (см. стр. 9) нажмите кнопку "Импортировать файл".
   На экране появится директория внутренней памяти устройства.
2. Укажите требуемый файл настроек и нажмите кнопку "Выбрать".
   На экране появится сообщение об успешном импорте настроек.
3. Нажмите кнопку "ОК".
   На экране появится главное окно приложения.

# Ручная настройка приложения в режиме TLS

Ручная настройка приложения выполняется с помощью файлов сертификатов, если отсутствует файл настроек. По требованию администратора пользователь создает на мобильном устройстве запрос на сертификат пользователя.

Администратор передает файлы сертификатов одним из следующих способов:

- пользовательский и корневой сертификаты ("user.cer" и "root.p7b");
- корневой сертификат ("root.p7b").

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

Перед выполнением импорта создайте папку в каталоге Клиента и разместите в ней полученные файлы.

## Создание запроса на сертификат

**Для создания запроса на сертификат:**

1. На экране предварительной настройки приложения (см. стр. **9**) нажмите кнопку "TLS".

   На экране появится окно выбора типа соединения.

2. Выберите требуемый тип соединения — сервер или ресурс.

   **Примечание.** Если выбран тип соединения "Ресурс", в окне "Сертификат" доступна кнопка "Пропустить", позволяющая сразу перейти к созданию ресурса (см. стр. **17**).

   На экране появится окно "Сертификат".

3. Нажмите кнопку "Запросить сертификат".

   На экране появится окно создания запроса на получение сертификата.

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

4. Укажите сведения о пользователе.

   **Примечание.** Тип запроса зависит от версии СД сервера доступа. Выпуск сертификатов по запросам типа "Для сервера доступа 3.X" должен осуществляться средствами СД соответствующих версий. В противном случае импорт таких сертификатов может завершиться ошибкой.

   В зависимости от выбранного типа субъекта обязательными являются поля, указанные ниже.

| 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 ФЛ** | | + | + | | + |
| **ИНН ЮЛ** | | | | | |
| **СНИЛС** | | + | | + | |
| **ОГРН** | | | + | | + |
| **ОГРНИП** | | | | + | |

5. Нажмите кнопку "Далее".

   На экране появится окно установки пароля доступа к ключевому контейнеру.

6. Введите пароль и подтвердите его в требуемых полях.

   **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.

7. Нажмите кнопку "Далее".

   В нижней части экрана появится меню.

8. Нажмите кнопку "Отправить".

   **Примечание.**
   - При нажатии кнопки "Сохранить" выполните пп. **9, 10**. После этого передайте файл запроса администратору.
   - Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи.

   На экране появится директория внутренней памяти устройства.

9. Укажите папку для сохранения файла запроса и нажмите кнопку "Выбрать" либо создайте новую, нажав кнопку "Создать папку".

10. В появившемся окне нажмите кнопку "ОК".

    На экране появится окно выбора способа отправки файла.

11. Выберите требуемый почтовый клиент.

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

12. Впишите адрес и отправьте письмо администратору.

13. После получения файлов сертификатов выполните их импорт (см. ниже).

## Импорт сертификата

**Для импорта сертификата:**

1. На экране предварительной настройки (см. стр. **9**) нажмите кнопку "TLS".
2. Выберите требуемый тип соединения — сервер или ресурс.

   **Примечание.** Если выбран тип соединения "Ресурс", в окне "Сертификат" доступна кнопка "Пропустить", позволяющая сразу перейти к созданию ресурса (см. стр. **17**).

3. В окне "Сертификат" нажмите кнопку "Импортировать сертификат".

   На экране появится окно импорта сертификатов и ключа.

4. Выберите требуемый пункт.

   На экране появится директория внутренней памяти устройства.

5. Выберите файл сертификата или архив, содержащий файлы сертификатов.
6. При необходимости повторите действия, описанные в пп. **2**, **3**.
7. Нажмите кнопку "Подтвердить".

   В зависимости от выбранного типа соединения на экране появится окно добавления сервера (см. ниже) или ресурса (см. стр. **17**).

## Добавление сервера или ресурса

**Для добавления сервера:**

1. В окне добавления сервера укажите значения параметров настроек сервера, приведенных ниже.

| **Адрес** |
|---|
| IP-адрес или DNS-имя TLS-сервера |
| **Имя сервера** |
| Наименование сервера для установления TLS-подключения |

| **Сертификат** |
| --- |
| При нажатии на строку параметра открывается окно выбора сертификата для подключения. Список доступных сертификатов представляет собой список импортированных пользовательских сертификатов |
| **Использовать сертификат по умолчанию** |
| При активации параметра имя сертификата по умолчанию появится в поле "Сертификат".<br>Значение по умолчанию — "ВЫКЛ". Доступно для активации после выбора сертификата пользователя в настройках TLS-режима (см. табл. на стр. **34**) |
| **Сохранить пароль** |
| Отвечает за сохранение пароля при установлении TLS-подключения. Значение по умолчанию — "ВКЛ".<br>При активации параметра после ввода пароля он будет сохранен, для сервера будет выполняться автоматическое обновление списка ресурсов. В противном случае обновление списка ресурсов будет возможно вручную после ввода пароля |

2. Нажмите кнопку "Добавить".

   На экране появится запрос ввода пароля доступа к ключевому контейнеру.

3. Введите пароль ключевого контейнера и нажмите кнопку "Подтвердить".

   **Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к ключевому контейнеру — 5.

   На экране появится сообщение об успешном добавлении сервера.

4. Нажмите кнопку "ОК".

   **Примечание.**
   - Если первичное установление соединения с TLS-сервером не будет выполнено из-за его недоступности, в строке с ним появится статус "Недоступен" и сервер будет отмечен как неактивный.
   - Если обновление TLS-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 автоматически загрузится список ресурсов. На экране появится окно указания уровня доверия для сертификата.

5. Нажмите на строку с текущим значением и выберите требуемое значение из раскрывающегося списка:
   - нажмите кнопку "Всегда".

     Доверие серверному сертификату будет подтверждено. Окно больше появляться не будет;
   - нажмите кнопку "На время текущего сеанса".

     Доверие серверному сертификату будет подтверждено до сброса всех соединений. Окно появится снова при следующем ручном обновлении ресурсов;
   - нажмите кнопку "Не доверять".

     Доверие серверному сертификату не будет подтверждено. Окно появится снова при следующем ручном обновлении ресурсов.

6. Нажмите кнопку "Подтвердить".

   На экране появится главное окно приложения (см. стр. **7**).

**Для добавления ресурса:**

1. В окне добавления ресурса укажите значения параметров настроек ресурса, приведенных ниже.

| **Адрес** |
| --- |
| IP-адрес или DNS-имя защищенного ресурса |
| **Имя ресурса** |
| Название ресурса для установления TLS-подключения |
| **Сертификат** |
| При нажатии на строку параметра открывается окно выбора сертификата для подключения. Список доступных сертификатов представляет собой список импортированных пользовательских сертификатов |
| **Порт** |
| Номер порта, используемого для установления TLS-подключения. Значение по умолчанию — 443 |

| **Описание** |
| --- |
| Описание ресурса |
| **Использовать сертификат по умолчанию** |
| При активации параметра имя сертификата по умолчанию появится в поле "Сертификат".<br>Значение по умолчанию — "ВЫКЛ". Доступно для активации после выбора сертификата пользователя в настройках TLS-режима (см. табл. на стр. **34**) |
| **Сохранить пароль** |
| Отвечает за сохранение пароля при установлении TLS-подключения. Значение по умолчанию — "ВКЛ".<br>При активированном параметре после ввода пароля он будет сохранен |

2. Нажмите кнопку "Добавить".
3. При необходимости введите пароль ключевого контейнера в появившемся окне и нажмите кнопку "Подтвердить".

**Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к ключевому контейнеру — 5.

На экране появится сообщение об успешном добавлении ресурса.

4. Нажмите кнопку "ОК".

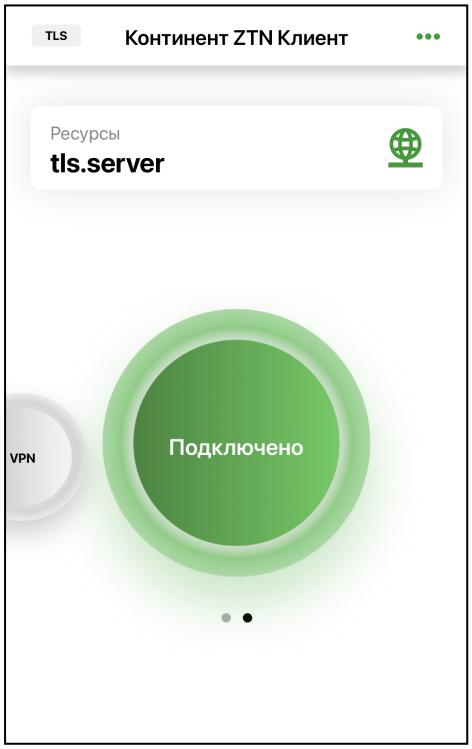
## Подключение к защищенному ресурсу в режиме TLS

### Для подключения к защищенному ресурсу в режиме TLS:

**Примечание.** При необходимости перед установлением TLS-подключения выполните настройку параметров приложения (см. стр. **33**).

1. В главном окне (см. стр. **7**) перейдите на страницу "TLS" и нажмите на индикатор подключения.

Индикатор подключения изменит цвет на зеленый.




При активном подключении разделы "Импортировать данные", "Сертификаты", "CDP", "CRL" и "Настройки" становятся недоступны.

2. Выберите панель "Ресурсы" и нажмите на строку веб-ресурса, к которому необходимо подключиться.

В браузере откроется страница выбранного веб-ресурса.

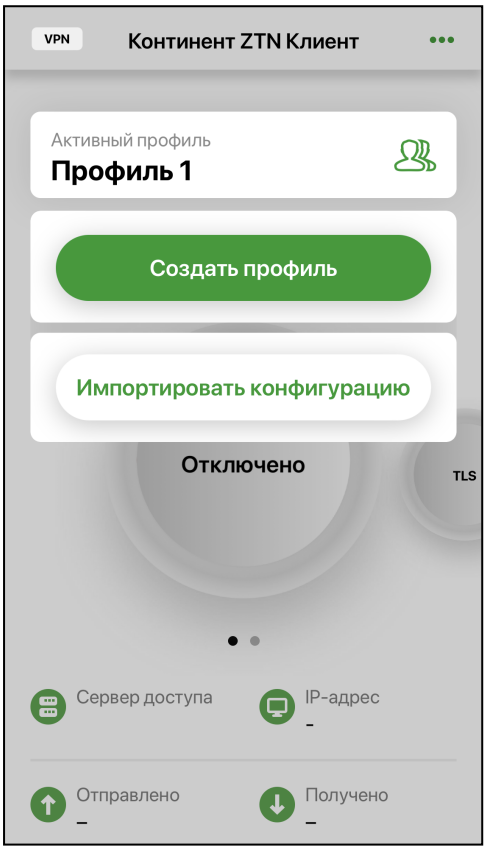
**Примечание.** При необходимости можно указать имя веб-ресурса в адресной строке браузера.

# Глава 3
# Эксплуатация

## Окно "Профили"

### Список профилей

Для перехода к списку профилей в главном окне на странице VPN выберите панель "Активный профиль". На экране появится список профилей.




**Для создания профиля:**

**Примечание.** Приложение поддерживает возможность создания профиля без привязки к сертификату. В зависимости от состояния параметра "Аутентификация по сертификату":

- параметр включен — профиль нельзя активировать, в списке он обозначается значком ⚠;
- параметр выключен — профиль может быть активирован (см. стр. 21) и использован для подключения к СД с помощью логина и пароля пользователя.

1. В списке профилей нажмите кнопку "Создать профиль".

   На экране появится окно создания профиля.

2. Укажите значения для параметров настроек профиля, приведенных ниже.

| **Имя профиля** |
|---|
| Наименование профиля для подключения к СД |
| **Сервер доступа** |
| IP-адрес или имя сервера доступа |

| **Прокси-сервер** |
| --- |
| При нажатии на строку открывается окно настройки прокси-сервера со следующими параметрами:<br>• адрес — IP-адрес или имя прокси-сервера;<br>• порт — порт прокси-сервера. Значение по умолчанию — 3128;<br>• аутентификация — тип аутентификации на прокси-сервере. Значение по умолчанию — "Без аутентификации" |
| **Сертификат** |
| Сертификат, используемый для подключения. При нажатии на строку параметра необходимо выбрать сертификат в раскрывающемся списке, содержащем импортированные ранее пользовательские сертификаты.<br>Доступно для настройки только при активированном параметре "Аутентификация по сертификату" |
| **Использовать прокси-сервер** |
| Значение по умолчанию — "ВЫКЛ". Доступно для активации после настройки параметров в окне "Прокси-сервер" |
| **Аутентификация по сертификату** |
| Тип аутентификации при подключении к СД. Значение по умолчанию — "ВКЛ". Зависит от типа сертификата в поле "Сертификат". При деактивации параметра аутентификация осуществляется по логину и паролю пользователя |
| **Сохранить пароль** |
| Отвечает за сохранение пароля при повторном подключении к СД. Значение по умолчанию — "ВЫКЛ". При активации параметра после ввода пароля он будет сохранен, окно запроса пароля больше появляться не будет |
| **Дополнительные настройки** |
| Доступны следующие дополнительные параметры для настройки профиля:<br>• порт сервера доступа (значение по умолчанию — 443);<br>• порт клиента — порт мобильного устройства. Значение по умолчанию — 7500;<br>• основной DNS-сервер, альтернативный DNS-сервер — по умолчанию используются адреса DNS-серверов, получаемые от СД. Если адреса не получены, их необходимо указать вручную. Адреса, полученные от СД, имеют приоритет над адресами, указанными вручную;<br>• домен — при необходимости можно указать DNS-суффикс, автоматически добавляемый к имени хоста при обращении к защищенным ресурсам;<br>• MTU — максимальный размер блока (в байт) на канальном уровне сети. Значение по умолчанию — 1500 |

3. Нажмите кнопку "Создать профиль".

   На экране появится сообщение об успешном создании профиля.
4. Нажмите кнопку "ОК".

   Профиль появится в списке.

### Для настройки профиля:

**Примечание.** Изменять настройки можно только для профиля, не используемого для активного подключения.

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

   В строке появятся кнопки настройки и удаления профиля.

2. Нажмите кнопку  .

   На экране появится окно настройки профиля.
3. Внесите исправления в доступные для редактирования поля.
4. Нажмите кнопку "Сохранить".

### Для удаления профиля:

**Внимание!** Удаление профиля, используемого для активного подключения, невозможно.

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

   В строке появятся кнопки настройки и удаления профиля.

2. Нажмите кнопку  .

   На экране появится запрос на удаление профиля.

3. Нажмите кнопку "Да".

   Профиль будет удален.

Для смены активного профиля выберите требуемый профиль в списке. Выбранный профиль отобразится на панели "Активный профиль".

## Импорт конфигурации

Импорт конфигурации осуществляется с использованием файла с расширением "*.apcfg" или "*.ts4", необходимого для подключения к СД версий 3.X или 4.X. После получения от администратора файла конфигурации создайте папку в каталоге Клиента и разместите в ней файл.

**Примечание.** Импорт конфигурации с использованием файлов с расширением "*.apcfg" поддерживается только для подключения к СД по протоколу версии 4.

**Для импорта конфигурации на панели "Активный профиль":**

**Примечание.** Сведения об импорте файла конфигурации при первом запуске приложения приведены на стр. 9.

1. В главном окне приложения на странице "VPN" выберите панель "Активный профиль".
2. В появившемся раскрывающемся списке нажмите кнопку "Импортировать конфигурацию".

   На экране появится директория внутренней памяти устройства.

3. Выберите полученный файл конфигурации, содержащийся в созданной ранее папке, нажав кнопку "Выбрать".

   На экране появится окно ввода пароля доступа к конфигурации.

4. Введите пароль к файлу конфигурации и нажмите кнопку "Подтвердить".

   **Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к файлу конфигурации или ключевому контейнеру — 5.

   На экране появится окно ввода пароля доступа к ключевому контейнеру.

5. При необходимости введите пароль к ключевому контейнеру и нажмите кнопку "Подтвердить".

   **Примечание.** В состав файла конфигурации может входить несколько ключевых контейнеров, профилей и т. д. Будет осуществлен импорт только первых в списке профиля, ключевого контейнера и т. д., остальные файлы будут проигнорированы.

   На экране появится сообщение об успешном импорте файла.

6. Нажмите кнопку "ОК".

   Сертификаты и ключевой контейнер будут извлечены в скрытую папку (подробнее см. на стр. **26**). Будет выполнен импорт сертификатов и создан новый профиль.

**Для импорта конфигурации в меню главного окна:**

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

   На экране появится окно выбора типа данных для импорта.

2. Нажмите кнопку "Импортировать конфигурацию".

   На экране появится директория внутренней памяти устройства.

3. Выполните действия, описанные выше в пп. **3–6**.

В случае повторного импорта конфигурации:

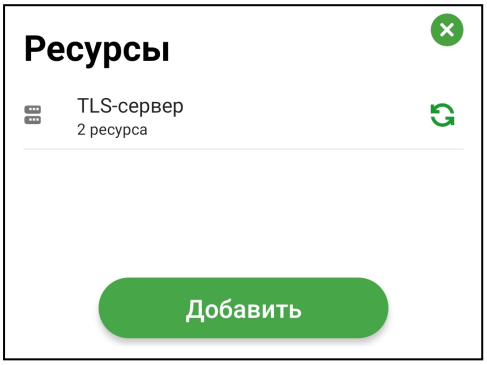
- старые сертификаты, ключевые контейнеры на устройстве и ссылки на сертификаты в приложении не удаляются;
- профиль из конфигурации добавится с именем <имя_профиля>-n, а старый профиль останется. При этом значение "n" представляет собой порядковый номер профиля, импортированного повторно;
- активный профиль не заменяется. Необходимо активировать новый профиль вручную, нажав на область "Активный профиль" и выбрав профиль из списка.

# Окно "Ресурсы"

## Список ресурсов

**Примечание.** Настройка списка ресурсов доступна только при неактивном TLS-режиме (индикатор подключения имеет серый цвет и надпись "Отключено").

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".
   На экране появится окно добавления сервера.
2. В окне добавления сервера укажите значения параметров настроек сервера, приведенных ниже.
3. Укажите значения параметров настроек сервера, приведенных ниже.

| |
|---|
| **Адрес** |
| Сетевое имя или IP-адрес сервера |
| **Имя сервера** |
| Наименование сервера для установления TLS-подключения |
| **Сертификат** |
| При нажатии на строку параметра открывается окно выбора сертификата для подключения. Список доступных сертификатов представляет собой список импортированных пользовательских сертификатов.<br>При активации параметра "Использовать сертификат по умолчанию" в поле "Сертификат" появится название сертификата, указанного в настройках TLS-режима как сертификат по умолчанию (см. табл. на стр. **34**) |
| **Использовать сертификат по умолчанию** |
| При активации параметра имя сертификата по умолчанию появится в поле "Сертификат". При выбора в поле "Сертификат" другого сертификата параметр "Использовать сертификат по умолчанию" будет деактивирован. Значение по умолчанию — "ВЫКЛ". Доступно для активации после выбора сертификата пользователя в настройках TLS-режима (см. табл. на стр. **34**) |
| **Сохранить пароль** |
| Отвечает за сохранение пароля при установлении TLS-подключения. Значение по умолчанию — "ВКЛ".<br>При активации параметра после ввода пароля он будет сохранен, для сервера будет выполняться автоматическое обновление списка ресурсов. В противном случае обновление списка ресурсов будет возможно вручную после ввода пароля |

4. Нажмите кнопку "Добавить".
   На экране появится запрос ввода пароля доступа к ключевому контейнеру.
5. Введите пароль ключевого контейнера и нажмите кнопку "Подтвердить".

   **Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к ключевому контейнеру — 5.

   На экране появится сообщение об успешном добавлении сервера.
6. Нажмите кнопку "ОК".

**Примечание.**
- Если первичное установление соединения с TLS-сервером не будет выполнено из-за его недоступности, в строке с ним появится статус "Недоступен" и сервер будет отмечен как неактивный.
- Если обновление TLS-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 автоматически загрузится список ресурсов. На экране появится окно указания уровня доверия для сертификата.

7. Нажмите на строку с текущим значением и выполните одно из следующих действий:
   - нажмите кнопку "Всегда".

     Доверие серверному сертификату будет подтверждено. Окно больше появляться не будет;
   - нажмите кнопку "На время текущего сеанса".

     Доверие серверному сертификату будет подтверждено до сброса всех соединений. Окно появится снова при следующем ручном обновлении ресурсов;
   - нажмите кнопку "Не доверять".

     Доверие серверному сертификату не будет подтверждено. Окно появится снова при следующем ручном обновлении ресурсов.
8. Нажмите кнопку "Подтвердить".

**Для добавления ресурса:**

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

   На экране появится окно добавления ресурса.
2. Укажите значения параметров настроек ресурса, приведенных ниже.

| |
|---|
| **Адрес** |
| Сетевое имя или IP-адрес ресурса |
| **Имя ресурса** |
| Название ресурса для установления TLS-подключения |
| **Сертификат** |
| При нажатии на строку параметра открывается окно выбора сертификата для подключения. Список доступных сертификатов представляет собой список импортированных пользовательских сертификатов.<br>При активации параметра "Использовать сертификат по умолчанию" в поле "Сертификат" появится название сертификата, указанного в настройках TLS-режима как сертификат по умолчанию (см. табл. на стр. **34**) |
| **Порт** |
| Номер порта, используемого для установления TLS-подключения. Значение по умолчанию — 443 |
| **Описание** |
| Описание ресурса |
| **Использовать сертификат по умолчанию** |
| При активации параметра имя сертификата по умолчанию появится в поле "Сертификат". При выбора в поле "Сертификат" другого сертификата параметр "Использовать сертификат по умолчанию" будет деактивирован. Значение по умолчанию — "ВЫКЛ". Доступно для активации после выбора сертификата пользователя в настройках TLS-режима (см. табл. на стр. **34**) |
| **Сохранить пароль** |
| Отвечает за сохранение пароля при установлении TLS-подключения. Значение по умолчанию — "ВКЛ".<br>При активированном параметре после ввода пароля он будет сохранен |

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

**Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к ключевому контейнеру — 5.

На экране появится сообщение об успешном добавлении ресурса.

5. Нажмите кнопку "ОК".

**Для настройки сервера/ресурса:**

1. В окне "Ресурсы" проведите пальцем справа налево по серверу/ресурсу.
   В строке появятся кнопки настройки и удаления сервера/ресурса.

2. Нажмите кнопку  .
   На экране появится окно редактирования сервера/ресурса.
3. Внесите необходимые изменения и нажмите кнопку "Сохранить".
   При добавлении/смене сертификата на экране появится запрос ввода пароля к ключевому контейнеру.
4. При необходимости введите пароль ключевого контейнера и нажмите кнопку "Подтвердить".

**Примечание.** Максимальное количество неудачных попыток ввода пароля доступа к ключевому контейнеру — 5.

Для обновления списка ресурсов в окне "Ресурсы" в строке с требуемым сервером нажмите кнопку  и введите пароль для ключевого контейнера. В области уведомлений устройства появится сообщение о результате выполнения операции. В случае успеха ресурсы сервера будут обновлены.

**Примечание.** В настройках TLS-режима по умолчанию активирован переключатель "Автоматическое обновление" (см. табл. на стр. 34).

**Для удаления сервера/ресурса:**

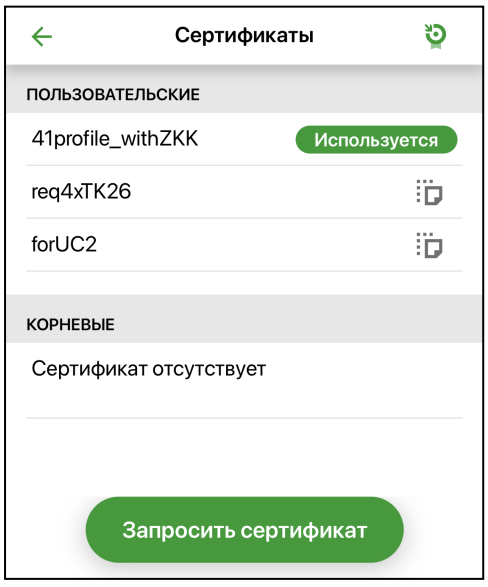
1. В окне "Ресурсы" проведите пальцем справа налево по серверу/ресурсу.
   В строке появятся кнопки настройки и удаления сервера/ресурса.

2. Нажмите кнопку  .
   На экране появится запрос на удаление ресурса.
3. Нажмите кнопку "Да".
   Сервер/ресурс будет удален.

# Окно "Сертификаты"

## Описание окна

Для работы с сертификатами в главном окне приложения вызовите меню и нажмите кнопку "Сертификаты". На экране появится окно "Сертификаты".



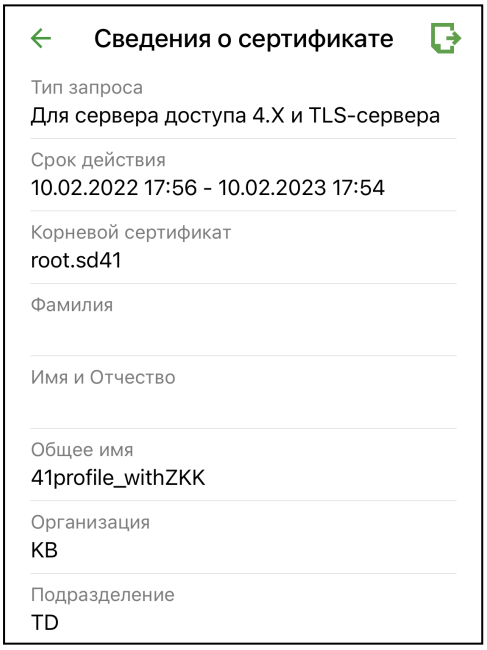
**Примечание.** Статус сертификата отсутствует в следующих случаях:
- сертификат не просрочен и прошел проверку по CRL;
- проверка по CRL отключена.

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 статусы, приведенные ниже.

| 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 или корневом сертификате выберите его в списке. На экране появятся сведения о сертификате.

**Примечание.** В качестве примера приведены сведения о сертификате пользователя.

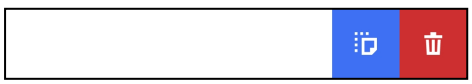



**Примечание.** Для просмотра информации о корневом сертификате, связанным с пользовательским, в окне "Сведения о сертификате" нажмите на строку "Корневой сертификат".

### Для удаления сертификата:

**Внимание!** Сертификаты, привязанные к профилям, ресурсам и/или серверам, удалить нельзя.

1. В окне "Сертификаты" проведите пальцем справа налево по строке с сертификатом.
   В строке появятся кнопки скрытия и удаления сертификата.



2. Нажмите кнопку  .
   На экране появится запрос на удаление сертификата.
3. Нажмите кнопку "Да".

**Для экспорта сертификата:**

1. В окне "Сертификаты" нажмите на строку с сертификатом.
   На экране появится окно со сведениями о сертификате.
2. Нажмите кнопку  .
   На экране появится окно выбора способа отправки файла.
3. Выберите требуемый почтовый клиент.
   В появившемся окне автоматически будут заполнены строки "От", "Тема" и вложен файл сертификата.
4. Введите адрес получателя и отправьте письмо.

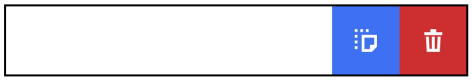
### Скрытие сертификатов

Процедура предназначена для защиты файлов от 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/настроек, а также файлов сертификатов все сертификаты импортируются скрытыми.

**Для скрытия файлов:**

1. В окне "Сертификаты" проведите пальцем справа налево по строке требуемого сертификата.
   В строке появятся кнопки скрытия и удаления сертификата.



2. Нажмите кнопку  .
   В строке со скрытым сертификатом появится значок  .

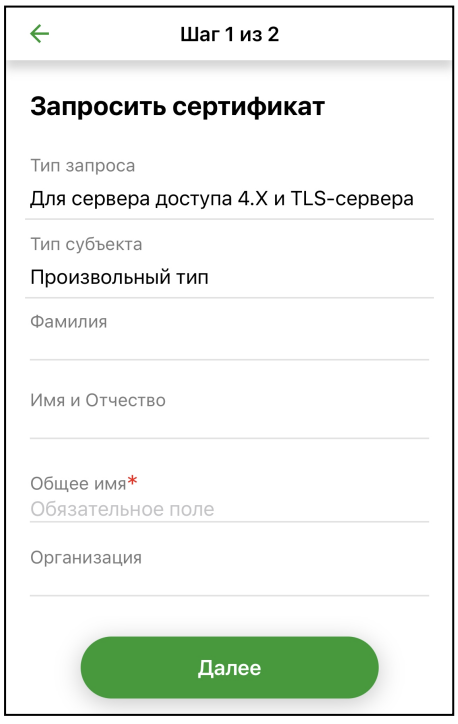
Для отмены операции скрытия выполните ее повторно, указав пустую директорию для сохранения файла.

## Меню окна "Сертификаты"

### Запрос на сертификат

**Для создания запроса на сертификат:**

1. В окне "Сертификаты" нажмите кнопку "Запросить сертификат".



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

2. Укажите сведения о пользователе.

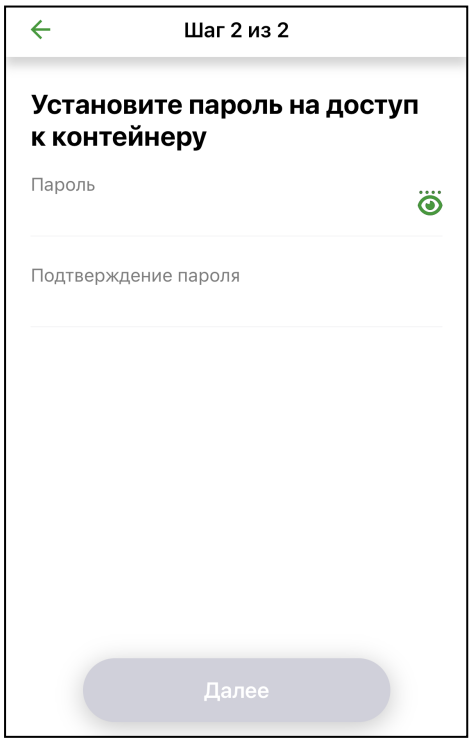
**Примечание.** Тип запроса зависит от версии СД. Выпуск сертификатов по запросам типа "Для сервера доступа 3.X" должен осуществляться средствами СД соответствующих версий. В противном случае импорт таких сертификатов может завершиться ошибкой.

В зависимости от выбранного типа субъекта обязательными являются поля, указанные ниже.

| 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 ФЛ** | | + | + | | + |
| **ИНН ЮЛ** | | | | | |
| **СНИЛС** | | + | | + | |
| **ОГРН** | | | + | | + |
| **ОГРНИП** | | | | + | |

3. Нажмите кнопку "Далее".

На экране появится окно установки пароля доступа к ключевому контейнеру.




4. Введите пароль и подтвердите его в требуемых полях.

**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.

5. Нажмите кнопку "Далее".

   В нижней части экрана появится меню.


6. Нажмите кнопку "Отправить".

**Примечание.**
- При нажатии кнопки "Сохранить" выполните пп. **7**, **8**. После этого передайте файл запроса администратору.
- Передача файлов запроса на получение сертификата пользователя может выполняться по открытым каналам связи.

   На экране появится директория внутренней памяти устройства.

7. Укажите папку для сохранения запроса на сертификат и нажмите кнопку "Выбрать" либо создайте новую, нажав кнопку "Создать папку".

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

**Внимание!** При удалении приложения с устройства файл ключевого контейнера также будет удален.

8. Нажмите кнопку "ОК".

   На экране появится окно выбора способа отправки файла.

9. Выберите требуемый почтовый клиент.

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

10. Впишите адрес и отправьте письмо администратору.

**Примечание.** Администратор передает файлы одним из следующих способов:
- пользовательский и корневой сертификаты;
- корневой сертификат.

### Импорт сертификатов и ключа

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

Импорт сертификатов возможен в следующих комбинациях:

- сертификат пользователя, ключевой контейнер в формате PKCS#15 и корневой сертификат;
- корневой сертификат.

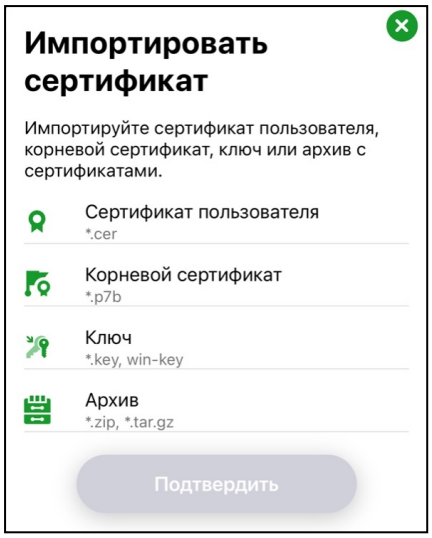
Перед выполнением импорта создайте папку в каталоге Клиента и разместите в ней полученные от администратора файлы сертификатов.

#### Для импорта сертификатов и ключа:

**Внимание!**
- При импорте сертификата пользователя необходимо предъявлять закрытый ключ, полученный с импортируемым сертификатом. В противном случае попытки установления соединения завершатся следующей ошибкой: "Неверный пароль ключевого контейнера, или сертификат пользователя не соответствует ключу".
- При импорте архива с сертификатами из почты убедитесь, что внутри архива нет других папок.

1. Выполните одно из следующих действий:
   - вызовите меню в окне "Сертификаты" и нажмите кнопку  ;
   - в главном окне приложения в меню нажмите кнопку "Импортировать данные", затем в появившемся окне нажмите кнопку "Импортировать сертификат".

На экране появится окно импорта сертификатов и ключа.




2. Выберите требуемый пункт.

   На экране появится директория внутренней памяти устройства.
3. Выберите файл сертификата или архив, содержащий файлы сертификатов.
4. При необходимости повторите действия, описанные в пп. **2**, **3**.
5. Нажмите кнопку "Подтвердить".

**Примечание.** Все сертификаты импортируются скрытыми и будут отображаться только в приложении. Для просмотра файлов сертификатов на устройстве отмените операцию скрытия файлов (подробнее см. на стр. 26).

6. В появившемся окне нажмите кнопку "ОК".

При импорте сертификатов, уже имеющихся во внутренней памяти устройства:

- если выбраны сертификат и ключ, ранее импортированные в приложение, их файлы не заменяются;
- если выбранный сертификат ранее импортирован в приложение, а файл ключа — новый, операция выполняется с заменой старого сертификата и ключа на новые.

## 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". На экране появится окно "CDP".

### Управление CDP

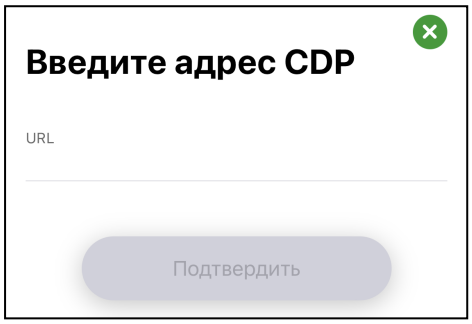
Если используемые сертификаты содержат информацию о CDP, приложение получит ее при импорте сертификатов (см. стр. **28**).

**Примечание.** Для сертификатов, выпущенных на СД, CRL не требуется. Для подключения к СД отключите проверку по CRL (подробнее см. на стр. 33).

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".
   На экране появится окно для ввода URL-адреса.




2. В поле "URL" введите адрес CDP в следующем формате:
   `http://[link].crl`
   где [link] — доменное имя требуемого ресурса.
3. Нажмите кнопку "Подтвердить".
   CDP будет добавлен в список.

**Для удаления CDP из списка:**

**Примечание.**
- CDP, полученные из сертификатов, нельзя удалить вручную. Такие CDP удаляются автоматически после удаления 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.
   В строке появятся кнопки настройки и удаления CDP.

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.
   В строке появятся кнопки настройки и удаления CDP.

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. **33**);
- 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 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". На экране появится окно "CRL".

**Примечание.**

- Работа с CRL в формате Base64 не поддерживается.
- 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. Укажите требуемый файл и нажмите кнопку "Выбрать".
   На экране появится соответствующее сообщение.
3. Нажмите кнопку "ОК".
   В списке появится новый CRL.

Для просмотра сведений о CRL в окне "CRL" выберите требуемую строку из списка. На экране появится окно со сведениями о CRL.


**Для отправки файла CRL:**

1. В окне "CRL" выберите требуемую строку из списка.
   На экране появится окно "Сведения о CRL".
2. Нажмите кнопку  .
   На экране появится окно выбора способа отправки файла.
3. Выберите требуемый почтовый клиент.
   В появившемся окне 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.
   В строке появятся кнопки настройки и удаления CRL.

2. Нажмите кнопку  .
   На экране появится запрос на удаление CRL.
3. Нажмите кнопку "Да".

**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 "Да".

# Окно "Настройки"

В окне выполняется настройка как общих параметров приложения, так и параметров установления соединения с СД и защищенными ресурсами в режимах работы VPN и TLS соответственно.

**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 параметров, приведенных ниже.

| Параметр | Описание |
|---|---|
| **Вкладка "Общие"** | |
| **Уведомлять об истечении срока действия сертификатов** | Настройка получения уведомлений об истечении срока действия сертификатов и закрытых ключей.<br>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 будет невозможно установить соединение с СД и ресурсами после окончания срока действия CRL.<br>Принимает значение от 0 до 30. Значение по умолчанию — 0 |
| **Автоматическая загрузка CRL** | Автоматическое обновление списка отозванных сертификатов в период времени, установленный параметром "Период загрузки CRL". Значение по умолчанию — "ВКЛ".<br>При выключенном параметре обновление CRL можно выполнить вручную в меню окна "CDP" (см. стр. **31**) |
| **Период загрузки CRL** | Периодичность обновления (в часах) списка отозванных сертификатов.<br>Принимает значение от 1 до 48. Значение по умолчанию — 12 |
| **Тип** | Уровень детализации журнала приложения.<br>Принимает одно из следующих значений:<br>• базовый (по умолчанию);<br>• расширенный |
| **Вкладка "VPN"** | |
| **Постоянное соединение** | Соединение, отключаемое только средствами настройки параметров VPN-подключения, автоматически восстанавливается после потери сетевого соединения. Для включения параметра предварительно настройте или активируйте профиль подключения (см. стр. **20**).<br>Значение по умолчанию — "ВЫКЛ".<br>Недоступно для управления, если активирован параметр "Переподключение" |
| **Переподключение** | Автоматическое переподключение при потере сетевого соединения или разрыве защищенного канала по инициативе сервера доступа АПКШ "Континент". Значение по умолчанию — "ВКЛ".<br>Недоступно для управления, если активирован параметр "Постоянное соединение" |
| **Количество попыток переподключения** | После последней неудачной попытки, количество которых задается пользователем, выводится сообщение об ошибке подключения.<br>Принимает значение от 1 до 99999. Значение по умолчанию — 3.<br>Доступно для управления только при активации параметра "Переподключение" |
| **Время ожидания переподключения** | Пауза (в секундах) между попытками подключения.<br>Принимает значение от 1 до 99999. Значение по умолчанию — 30.<br>Доступно для управления только при активации параметра "Переподключение" |

| Параметр | Описание |
|---|---|
| **Время ожидания при бездействии** | Время неактивности (в секундах), по истечении которого произойдет отключение от СД. Под неактивностью понимается отсутствие трафика в защищенном канале.<br>Принимает значение от 1 до 99999. Значение по умолчанию — 600.<br>Доступно для управления только при активации параметра "Переподключение" |
| **Соединение по запросу** | При активации параметра появится уведомление о необходимости выполнения тестового подключения. Это требуется для того, чтобы Клиент получил список защищенных ресурсов от СД, как только пользователь выполнит аутентификацию.<br>Соединение с СД устанавливается в случае попытки установки соединения с ресурсом, DNS-имя которого не удалось разрешить.<br>Если пароль ключевого контейнера или учетные данные (логин и пароль) не были<br>сохранены ранее, при подключении к СД пользователь получит уведомление о необходимости перехода в приложение для выполнения аутентификации.<br>Значение по умолчанию — "ВЫКЛ".<br>Недоступно для управления, если активирован один из параметров "Постоянное соединение" или "Переподключение" |
| **Максимальное время бездействия** | Время неактивности (в секундах), по истечении которого прекратится установление соединения с СД.<br>Принимает значение от 1 до 99999. Значение по умолчанию — 120.<br>Доступно для управления только при активации параметра "Соединение по запросу" |
| **Вкладка "TLS"** | |
| **Сертификат по умолчанию** | Сертификат пользователя, используемый по умолчанию для подключения к защищенным ресурсам. При нажатии на область появляется список импортированных ранее сертификатов |
| **Подтверждать сброс соединений** | Активируйте параметр, если необходимо подтверждать сброс соединений. Значение по умолчанию — "ВКЛ" |
| **Протокол TLS** | Версии используемого TLS-протокола. Принимает одно из следующих значений:<br>• TLS 1.0 и TLS 1.2 (по умолчанию);<br>• TLS 1.0;<br>• TLS 1.2 |
| **Использовать шифронаборы** | Активируйте параметр, если необходимо использовать шифронаборы. Значение по умолчанию — "ВКЛ" |
| **Шифронабор "Магма"** | Управление использованием шифронаборов "Магма" и "Кузнечик".<br>Значение по умолчанию — "ВКЛ".<br>Доступны для управления только при активации параметра "Использовать шифронаборы" |
| **Шифронабор "Кузнечик"** | |
| **Автоматическое обновление** | Автоматическое обновление списка ресурсов, загружаемых с сервера. Значение по умолчанию — "ВКЛ".<br>При отключенном параметре обновление списка ресурсов можно выполнить вручную с помощью панели "Ресурсы" (см. стр. **24**) |
| **Период обновления** | Период обновления (в часах) списка ресурсов, загружаемых с сервера.<br>Принимает значение от 1 до 48. Значение по умолчанию — 12.<br>Доступно для управления только при активации параметра "Автоматическое обновление" |

**3.** Нажмите кнопку "Сохранить".

Внесенные изменения будут применены.

## Экспорт настроек

Экспорт настроек предназначен для сохранения пакета настроек в файл с расширением "*.csf" для последующего переноса профилей, сертификатов и ключевых контейнеров, серверов и ресурсов, настроек приложения на новое устройство.

**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 директория внутренней памяти устройства.
3. Укажите папку для сохранения файла и нажмите кнопку "Выбрать".

   На экране появится сообщение об успешном выполнении операции.
4. 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 (см. ниже).

## Импорт настроек

Операция предназначена для установки пакета настроек из приложения, установленного на другом устройстве. В результате успешного импорта все настройки (профили, сертификаты и т. д.) будут перезаписаны. Для получения файла настроек требуется выполнить операцию экспорта (см. выше). Перед выполне-нием импорта создайте папку в каталоге Клиента и разместите в ней файл настроек с расширением "*.csf".

**Для импорта настроек:**

**Примечание.** Сведения об импорте файла настроек при первом запуске приложения в режиме VPN приведены на стр. 10, в режиме TLS — на стр. 14.

1. Выполните одно из следующих действий:
   - в главном окне приложения в меню нажмите кнопку "Настройки", затем в меню в окне "Настройки" нажмите кнопку "Импортировать настройки";
   - в главном окне приложения в меню нажмите кнопку "Импортировать данные", затем в появившемся окне нажмите кнопку "Импортировать настройки".

   На экране появится директория внутренней памяти устройства.
2. Укажите требуемый файл настроек и нажмите кнопку "Выбрать".

   На экране появится сообщение об успешном импорте настроек.
3. Нажмите кнопку "ОК".

   На экране появится главное окно приложения.

# Управление режимом работы

Континент ZTN Клиент функционирует в режимах, приведенных ниже.

### Основной режим

Режим по умолчанию. Пользователю предоставляются права полного доступа, включающие в себя:

- 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 настройка его параметров;
- просмотр списка серверов и ресурсов;
- просмотр и обновление ресурсов, загруженных с сервера;
- добавление и удаление сервера/ресурса;
- настройка параметров сервера/ресурса;
- импорт конфигурации;

- импорт/экспорт настроек;
- 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 и отправка журнала;
- просмотр сведений о Клиенте в окне "О программе";
- контроль целостности.

### Режим ограниченной функциональности

Пользователю предоставляются права ограниченного доступа к управлению настройками приложения, включающие в себя:

- подключение/отключение к/от СД в режиме работы VPN;
- установление и разрыв соединений с защищенными ресурсами в режиме работы TLS;
- просмотр и отправка журнала;
- просмотр сведений о Клиенте в окне "О программе";
- контроль целостности.

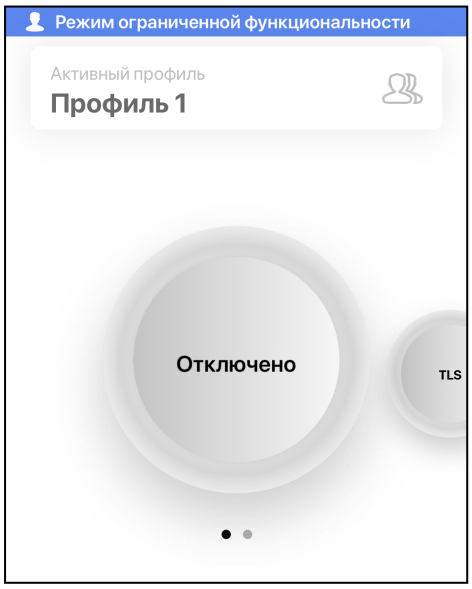
### Изменение режима работы

**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 требуемых полях, и нажмите кнопку "Подтвердить".

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




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

# Журнал

## Журнал работы приложения

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

Для работы с журналом в главном окне приложения вызовите меню и нажмите кнопку "Журнал". На экране появится журнал работы приложения.


В журнале предусмотрены два уровня детализации: базовый и расширенный. Настройка уровня детализации выполняется в окне "Настройки" (см. стр. **33**).

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, а красный — для событий, связанных с ошибками.

| Уровень детализации | Цвет | Событие |
|---|---|---|
| Базовый | Черный | Континент ZTN Клиент запущен |
| Базовый | Черный | Добавлен защищенный ресурс |
| Базовый | Черный | Удален защищенный ресурс |
| Базовый | Черный | Добавлен профиль |
| Базовый | Черный | Удален профиль |
| Базовый | Черный | Файл настроек успешно импортирован |
| Базовый | Черный | Файл конфигурации успешно импортирован |
| Базовый | Черный | Параметры подключения к СД изменены |
| Базовый | Черный | Пользователь инициировал попытку подключения к СД |
| Базовый | Черный | Соединение с СД разорвано |
| Базовый | Черный | Корневой сертификат добавлен в хранилище |
| Базовый | Черный | Корневой сертификат удален |
| Базовый | Черный | Пользовательский сертификат добавлен в хранилище |
| Базовый | Черный | Пользовательский сертификат удален |

| Уровень детализации | Цвет | Событие |
|---|---|---|
| Базовый | Черный | Настройки проверки сертификатов изменены |
| Базовый | Черный | CRL успешно импортирован |
| Базовый | Черный | Добавлен CDP |
| Базовый | Черный | Отредактированы параметры CDP |
| Базовый | Зеленый | Установлено соединение с СД |
| Базовый | Зеленый | Установлено соединение с защищенным ресурсом |
| Базовый | Красный | Системная ошибка |
| Базовый | Красный | Не удалось проверить автоматическое обновление списка ресурсов TLS-сервера |
| Базовый | Красный | Нарушена целостность файла! Создание новых сессий запрещено |
| Базовый | Красный | Для сертификата не найден соответствующий CRL |
| Базовый | Красный | СД разорвал соединение с Континент ZTN Клиент |
| Расширенный | Черный | Изменен пароль доступа к ключевому контейнеру сертификата |
| Расширенный | Черный | Выполнено автоматическое конфигурирование перечня ресурсов |
| Расширенный | Черный | Выполнен перерасчет контрольной суммы файла |
| Расширенный | Черный | Выполнена загрузка CRL |
| Расширенный | Зеленый | Континент ZTN Клиент успешно установлен |
| Расширенный | Зеленый | Инициализация процедуры проверки целостности файлов выполнена успешно |
| Расширенный | Зеленый | Проверка целостности файла выполнена успешно |
| Расширенный | Зеленый | Самотестирование криптографических функций выполнено успешно |
| Расширенный | Красный | СД не отвечает |
| Расширенный | Красный | Выполнен сброс всех соединений |
| Расширенный | Красный | СД разорвал соединение во время аутентификации |
| Расширенный | Красный | Ошибка инициализации процедуры проверки целостности файлов Континент ZTN Клиент. Необходимо переустановить приложение |
| Расширенный | Красный | Целостность Континент ZTN Клиент нарушена! Создание новых сессий запрещено |
| Расширенный | Красный | Срок действия закрытого ключа для сертификата истекает через N дней. Установление соединения с СД/TLS-сервером/защищенным ресурсом будет невозможно! |
| Расширенный | Красный | Срок действия закрытого ключа для сертификата истек. Установление соединения с СД/TLS-сервером/защищенным ресурсом невозможно! |
| Расширенный | Красный | Срок действия сертификата истекает через N дней. Установление соединения с СД/TLS-сервером/защищенным ресурсом будет невозможно! |
| Расширенный | Красный | Не удалось установить соединение с СД/TLS-сервером/защищенным ресурсом. Срок действия сертификата еще не наступил |
| Расширенный | Красный | Не удалось установить соединение с СД/TLS-сервером/защищенным ресурсом. Срок действия сертификата истек |
| Расширенный | Красный | Пароль устарел. Необходимо изменить пароль для доступа к ключевому контейнеру |
| Расширенный | Красный | Срок действия энтропии для инициализации ДСЧ истек. Необходимо импортировать файл конфигурации или ключевой контейнер, содержащий источник энтропии |
| Расширенный | Красный | Ошибка подключения: истек срок действия закрытого ключа сертификата |
| Расширенный | Красный | Ошибка подключения: использован не поддерживаемый на СД режим организации VPN-соединения |

| Уровень детализации | Цвет | Событие |
|---|---|---|
| Расширенный | Красный | Установление соединения с профилем/TLS-сервером/защищенным ресурсом невозможно. Необходимо импортировать файл конфигурации или ключевой контейнер, содержащий seed |
| Расширенный | Красный | Работа приложения завершена с ошибкой |
| Расширенный | Красный | Не удалось ввести пароль для доступа к ключевому контейнеру сертификата |
| Расширенный | Красный | Не удалось ввести логин и/или пароль пользователя |
| Расширенный | Красный | Неверные логин и/или пароль. Количество попыток ввода логина и пароля исчерпано |
| Расширенный | Красный | Неверный пароль доступа к ключевому контейнеру. Количество попыток ввода пароля доступа к ключевому контейнеру исчерпано |

**Для отправки журнала:**

1. В окне "Журнал" вызовите меню и нажмите кнопку "Отправить журнал".
   На экране появится запрос на сохранение журнала.
2. Нажмите кнопку "Да".
   На экране появится директория внутренней памяти устройства.
3. Укажите папку для сохранения файла журнала и нажмите кнопку "Выбрать".
   На экране появится сообщение об успешном выполнении операции.
4. Нажмите кнопку "ОК".
   На экране появится окно выбора способа отправки файла.
5. Выберите требуемый почтовый клиент.
   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".
   На экране появится директория внутренней памяти устройства.
2. Укажите папку для сохранения файла журнала и нажмите кнопку "Выбрать".
   На экране появится сообщение об успешном выполнении операции.
3. Нажмите кнопку "ОК".
   На экране появится окно выбора способа отправки файла.
4. Выберите требуемый почтовый клиент.
   В окне почтового клиента автоматически будут заполнены строки "От", "Тема" и вложен файл журнала.
5. Впишите адрес и отправьте письмо администратору.

# Окно "О программе"

Окно "О программе" содержит сведения о текущей версии ПО "Континент ZTN Клиент" и статусе контроля целостности по результатам проверки контрольных сумм динамических библиотек, а также позволяет связаться со службой технической поддержки.

**Примечание.** Подробнее о выполнении проверки целостности см. на стр. 40.

Для обращения в службу технической поддержки по номеру телефона нажмите кнопку "Позвонить" и выполните вызов по указанному номеру.

**Для обращения в службу поддержки с помощью электронной почты:**

1. Нажмите кнопку "Написать".

   На экране появится окно выбора способа отправки файла.
2. Выберите требуемый почтовый клиент.

   В появившемся окне автоматически будут заполнены строки "От", "Тема" и вложен файл отладочного журнала.
3. Впишите адрес и отправьте письмо.

**Примечание.** Связаться со службой технической поддержки можно по электронной почте support@securitycode.ru.

## Контроль целостности

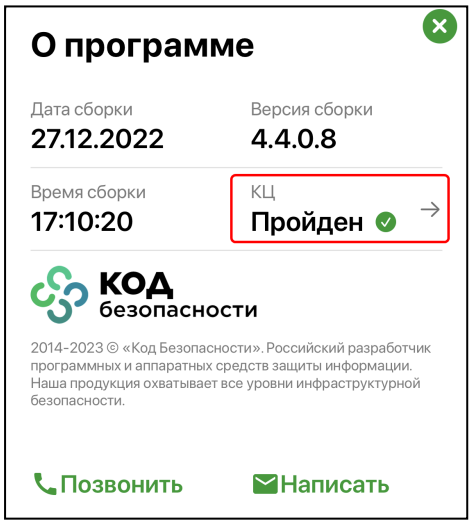
Контроль целостности файлов заключается в сравнении текущих значений контрольных сумм с эталонными значениями контрольных сумм динамических библиотек, заранее вычисленных при установке приложения на устройстве.

Контроль целостности приложения осуществляется:

- при каждом запуске приложения;
- перед подключением к СД;
- 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.




   На экране появится 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.