КОД безопасности

Континент ZTN Клиент для iOS, iPadOS

Начало работы

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**

Установка и первый запуск приложения

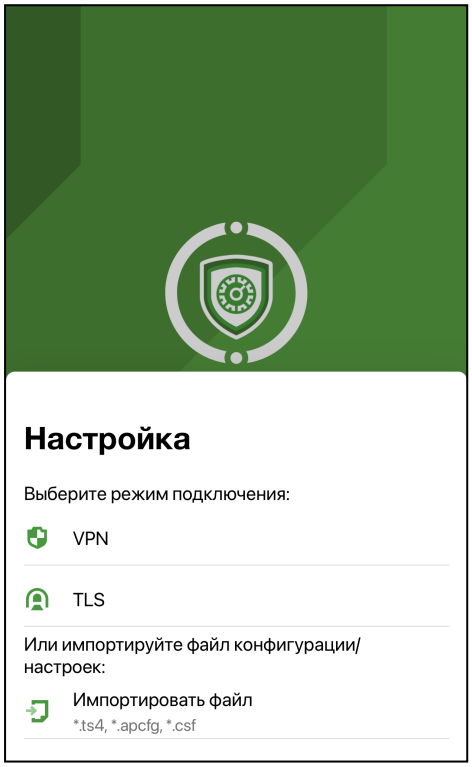
Установка приложения выполняется пользователем из магазина приложений App Store.

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.

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.

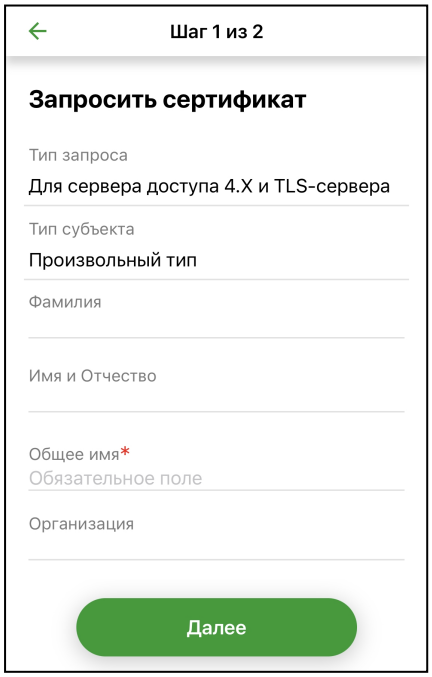
Перед выполнением импорта создайте папку в каталоге Клиента и разместите в ней полученные файлы.

Создание запроса на сертификат

Для создания запроса на сертификат:

1. На экране предварительной настройки (см. стр. **3**) 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 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.

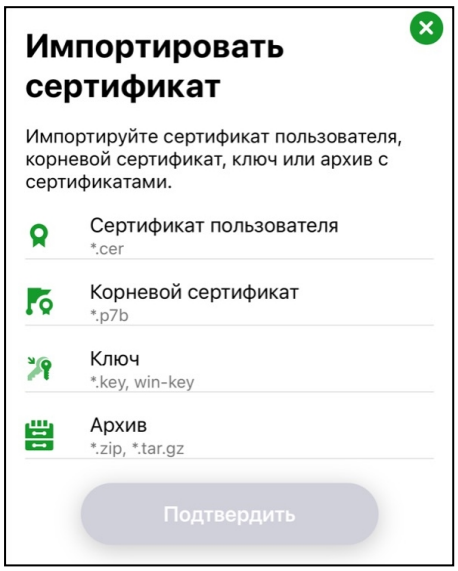
11. Впишите адрес и отправьте письмо администратору.

12. После получения файлов сертификатов выполните их импорт (см. стр. **6**).

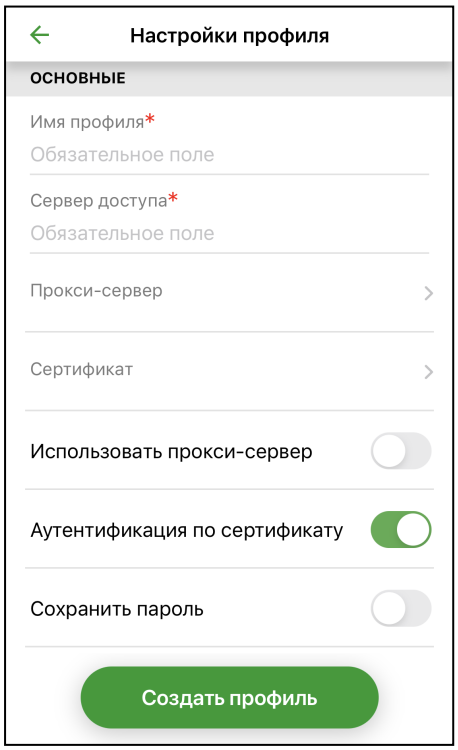
Импорт сертификатов

Для импорта сертификатов:

1. На экране предварительной настройки приложения (см. стр. 3) 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: • адрес — IP-адрес или имя прокси-сервера; • порт — порт прокси-сервера. Значение по умолчанию — 3128; • 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. 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: • порт сервера доступа (значение по умолчанию — 443); • порт клиента — порт мобильного устройства. Значение по умолчанию — 7500; • основной DNS-сервер, альтернативный DNS-сервер — по умолчанию используются адреса DNS-серверов, получаемые от СД. Если адреса не получены, их необходимо указать вручную. Адреса, полученные от СД, имеют приоритет над адресами, указанными вручную; • домен — при необходимости можно указать DNS-суффикс, автоматически добавляемый к имени хоста при обращении к защищенным ресурсам; • 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 .

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 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.

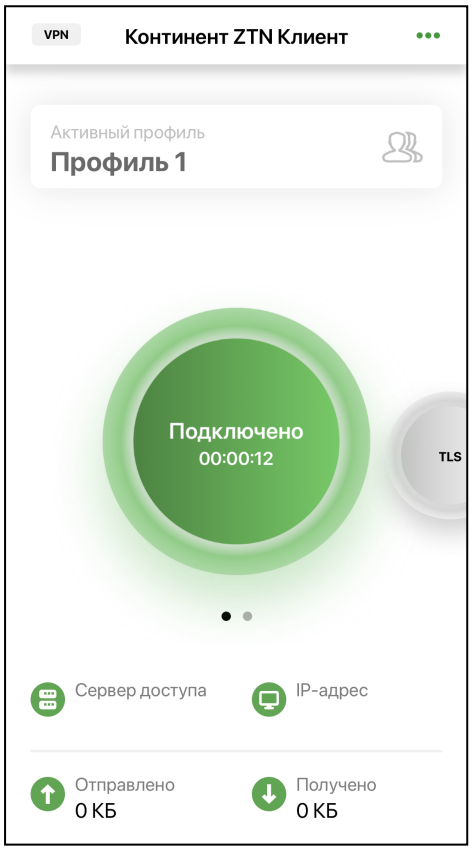
4. Введите пароль доступа к ключевому контейнеру и нажмите кнопку "Подтвердить".

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. 3) 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. **3**) 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. **11**).

   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 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. **3**) 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. 11).

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. **11**).

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". Значение по умолчанию — "ВЫКЛ". Доступно для активации после выбора сертификата пользователя в настройках TLS-режима
Сохранить пароль
Отвечает за сохранение пароля при установлении TLS-подключения. Значение по умолчанию — "ВКЛ". 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.

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". Значение по умолчанию — "ВЫКЛ". Доступно для активации после выбора сертификата пользователя в настройках TLS-режима
Сохранить пароль
Отвечает за сохранение пароля при установлении TLS-подключения. Значение по умолчанию — "ВКЛ". 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".

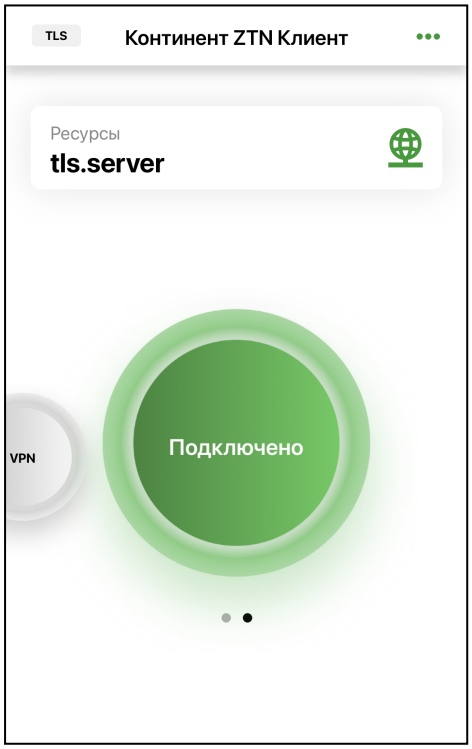
Подключение к защищенному ресурсу в режиме TLS

Для подключения к защищенному ресурсу в режиме TLS:

Примечание. При необходимости перед установлением TLS-подключения выполните настройку параметров приложения.

1. В главном окне 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.