КОД безопасности

Континент ZTN Клиент для Windows

Руководство по эксплуатации

АМБС.26.20.40.140.002 91

Почтовый адрес:	**115127, Россия, Москва, а/я 66 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

КС	Контрольная сумма
КЦ	Контроль целостности
МК	Менеджер конфигурации
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СД	Сервер доступа
СЗИ	Средство или система защиты информации
СКЗИ	Средство криптографической защиты информации
УКЦ	Утилита "Контроль целостности – Континент ZTN Клиент"
УЦ	Удостоверяющий центр
CDP	CRL Distribution Point
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DNS	Domain Name System
IP	Internet Protocol
NTLM	NT LAN Manager
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

Введение

Руководство предназначено для пользователей и администраторов изделия "Континент ZTN Клиент для Windows" АМБС.26.20.40.140.002 (далее — Континент ZTN Клиент, Клиент, изделие). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации изделия на базе ОС Windows.

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 "Код Безопасности" 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

Континент ZTN Клиент — программное средство, функционирующее в среде ОС Windows и реализующее следующие основные функции:

- установление защищенного соединения с сервером доступа изделия "Аппаратно-программный комплекс шифрования "Континент" версии 3.9 и узлом безопасности с включенным компонентом "Сервер доступа" изделия "Комплекс безопасности "Континент". Версия 4" (далее — комплекс "Континент");
- установление защищенного соединения с изделиями "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее — TLS-сервер), "Средство криптографической защиты информации "Криптографический сетевой программный комплекс "КриптоПро NGate" версия 1.0 R2" (далее — NGate), а также обмен данными с веб-серверами корпоративной сети;
- регистрация событий, связанных с функционированием Клиента;
- контроль целостности ПО Клиента и среды функционирования, передаваемой и хранимой информации.

Внимание!

Для установления защищенного соединения с NGate с использованием сертификата, сформированного средствами криптопровайдера "Код Безопасности CSP", необходимо в настройках Клиента на вкладке "TLS" указать сертификат по умолчанию. В других случаях требуется изделие "Средство криптографической защиты информации "КриптоПро CSP" версии 4.0/5.0 (далее — КриптоПро CSP), функционирующее совместно с Клиентом.

Континент ZTN Клиент имеет технические характеристики, приведенные ниже.

Алгоритм шифрования
В соответствии с ГОСТ 28147-89 и ГОСТ Р 34.12-2015
Защита передаваемых данных от искажения
В соответствии с ГОСТ 28147-89 и ГОСТ Р 34.12-2015 в режиме выработки имитовставки
Расчет хэш-функции
В соответствии с ГОСТ Р 34.11-2012
Формирование и проверка электронной подписи
В соответствии с ГОСТ Р 34.10-2012
Двусторонняя аутентификация
С использованием сертификатов X.509v3

Системные требования

Континент ZTN Клиент устанавливается на компьютеры, удовлетворяющие аппаратным и программным требованиям, приведенным ниже.

Элемент	Требование
Операционная система	• Windows 10 x86/x64 (не ниже версии 1909); • Windows 11 x64; • Windows Server 2016 x64; • Windows Server 2019 x64
Процессор, оперативная память	В соответствии с установленной ОС
Жесткий диск (свободное место)	300 Мбайт
Привод	Привод DVD/CD-ROM
Дополнительное ПО (при необходимости)	• ПАК "Соболь"; • СЗИ Secret Net Studio; • КриптоПро CSP; • Валидата CSP

Принципы функционирования

Режим VPN

Континент ZTN Клиент в режиме VPN осуществляет установление защищенного соединения с СД комплекса "Континент" через общедоступные (незащищенные) сети.

Для подключения к СД выполняется настройка параметров подключения. В зависимости от требований, предъявляемых к доступу удаленных пользователей к защищаемым ресурсам, на Клиенте может использоваться произвольное количество подключений, каждое из которых имеет индивидуальную настройку параметров и сохраняется в виде профиля подключения. Если в состав защищаемой сети входят несколько СД, соединение с каждым из них в рамках одного профиля подключения возможно при наличии сформированного списка доступных СД в настройках этого профиля.

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

При подключении к СД выполняется процедура установления соединения в соответствии с протоколом TLS, в ходе которой происходит взаимная аутентификация Клиента и СД. Процедура установления соединения завершается генерацией сеансового ключа, который используется для шифрования трафика.

Генерация закрытого ключа и формирование на его основе открытого при создании запроса на получение сертификата удостоверяющего центра выполняются средствами криптопровайдера.

Блокировка трафика до и после установления соединения с СД

Континент ZTN Клиент поддерживает режим работы, при котором до установления соединения с СД и после разрыва соединения на компьютере будет заблокирован весь сетевой трафик. Функционирование режима блокировки трафика не прерывается в случаях разрыва соединения с СД, завершения работы ПО Клиента и перезагрузки ОС.

Для включения такого режима работы необходимо настроить параметры блокировки трафика в свойствах пользователя в базе СД комплекса "Континент", а в настройках Клиента на вкладке "VPN" активировать параметр "Блокировать трафик до установления соединения с СД".

По умолчанию параметр "Блокировать трафик до установления соединения с СД":

- выключен в исполнениях Клиента, соответствующих классу КС1;
- включен в исполнениях Клиента, соответствующих классам КС2 и КС3.

Примечание.

- В исполнениях Клиента, соответствующих классу КС3, параметр "Блокировать трафик до установления соединения с СД" скрыт и включен всегда.
- Трафик не блокируется сразу после установки Клиента любого исполнения и до первого подключения к СД.
- Доступ кTLS-ресурсам в данном режиме не блокируется.

При активации параметра "Блокировать трафик до установления соединения с СД" для настройки становится доступен параметр "Применять новые настройки блокировки трафика при смене СД", при включении которого Клиент будет получать параметры блокировки трафика от каждого СД, с которым устанавливается соединение. Параметры, полученные от СД предыдущего соединения, не применяются.

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 шифрования, соответствующих ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015.

Для подключения к защищаемым веб-ресурсам корпоративной сети удаленный пользователь должен 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", используя сертификаты открытых ключей.

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

В случае невыполнения требований, предъявляемых к аутентификации Клиента и TLS-сервера, защищенное соединение не устанавливается и доступ пользователя к веб-ресурсу блокируется.

Сертификаты открытых ключей

Сертификат — это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется цифровой подписью удостоверяющего центра сертификации.

Поддерживается работа с ключами форматов стандарта PKCS#15 и сертификатами форматов кодирования DER, PEM, Base64.

Для работы Клиента требуются сертификаты, приведенные ниже.

Сертификат сервера доступа
Для подтверждения подлинности СД, взаимодействующего с Клиентом
Сертификат TLS-сервера
Для подтверждения подлинности TLS-сервера, взаимодействующего с Клиентом
Сертификат удаленного пользователя
Для аутентификации пользователя на СД/TLS-сервере
Корневой сертификат
Для подтверждения подлинности сертификатов СД, TLS-сервера и сертификата пользователя

Пользователь получает сертификаты от администратора безопасности любым защищенным способом или на основании созданного им запроса. Запрос на получение сертификата создается средствами Клиента. Одновременно с запросом формируется закрытый ключ пользователя. Запрос в виде файла сохраняется в указанную пользователем директорию, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе.

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.

Клиент автоматически отслеживает состояние сертификатов, осуществляя следующие проверки:

- по сроку действия сертификата;
- по CRL;

  Примечание.
  Для подключения с использованием сертификатов, выпущенных ПУ СД/МК, необходимо отключить проверку по CRL (см. стр. 39).

- путем построения цепочки сертификатов.

eXtended Container

Утилита eXtended Container (далее — XC) позволяет Клиенту работать с ключами, сформированными средствами СКЗИ "КриптоПро CSP", если КриптоПро CSP не установлено на компьютере, на котором функционирует Клиент. Для работы утилиты необходимо ввести лицензионный ключ для расширенной поддержки ключевых контейнеров при установке Клиента (см. стр. 11).

Внимание!
Если Континент ZTN Клиент был установлен без указания лицензии eXtended Container, для работы утилиты необходимо удалить ПО Клиента и криптопровайдер "Код Безопасности CSP", а затем — осуществить установку Клиента, указав лицензионный ключ XC.

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения и передачи пользователю ключевой информации — контейнера с закрытым ключом и пароля к нему.

В качестве ключевых носителей могут использоваться USB-флеш-накопители, реестр ОС Windows и аппаратные носители, типы которых приведены ниже.

USB-ключи и смарт-карты
• Рутокен Lite; • Рутокен ЭЦП 2.0; • Рутокен ЭЦП 2.0 Flash; • Рутокен S; • Esmart Token (смарт-карта); • Esmart Token ГОСТ; • JaCarta PKI; • JaCarta PKI/ГОСТ; • JaCarta-2 ГОСТ

Для использования аппаратных носителей требуется установка соответствующих драйверов и сопутствующего ПО.

Контроль целостности

Функция контроля целостности предназначена для слежения за неизменностью содержимого файлов установленного ПО Клиента и связанных с ним файлов ОС Windows. КЦ осуществляется с помощью утилиты "Контроль целостности – Континент ZTN Клиент", входящей в дистрибутив Клиента.

Выполняется сравнение текущих значений контрольных сумм контролируемых файлов и эталонных значений, рассчитанных в ходе установки Клиента. Процедура пересчета эталонных значений доступна пользователю с правами администратора ОС Windows.

Список файлов ПО, подлежащих контролю, и значения их контрольных сумм хранятся в конфигурационном файле. Конфигурационный файл формируется при установке установочного пакета.

КЦ установленного ПО осуществляется:

- при входе в систему (вне зависимости от значения параметра "Открывать Континент ZTN Клиент при запуске системы);
- при запуске Клиента;
- при установлении соединения с СД и защищенными веб-ресурсами;
- вручную, с помощью УКЦ;
- по расписанию, настраиваемому с помощью УКЦ (по умолчанию в воскресенье в 00:00 по системному времени).

Если в ходе проведения КЦ будет обнаружена ошибка, пользователь получит информационное сообщение о нарушении целостности.

Если в ходе проведения регламентной проверки целостности будет обнаружено нарушение целостности либо отсутствие контролируемого ПО, а Клиент будет активным, рабочие сессии с защищенными ресурсами продолжатся. Установление соединения с СД и создание новых сессий будут заблокированы.

В случае обнаружения нарушения целостности при неактивном ПО Клиента будет сделана соответствующая запись в журнале событий.

При нарушении целостности сообщение о необходимости ее восстановления будет показываться пользователю:

- при каждом запуске Клиента;
- при каждой попытке установления соединения с СД и защищенными веб-ресурсами (если нарушение целостности обнаружено в ходе регламентного контроля целостности при наличии активного соединения).

Если Континент ZTN Клиент используется совместно с ПАК "Соболь", дополнительно проверка контрольных сумм выполняется при загрузке операционной системы. Результаты проверки заносятся в журнал событий.

Аудит

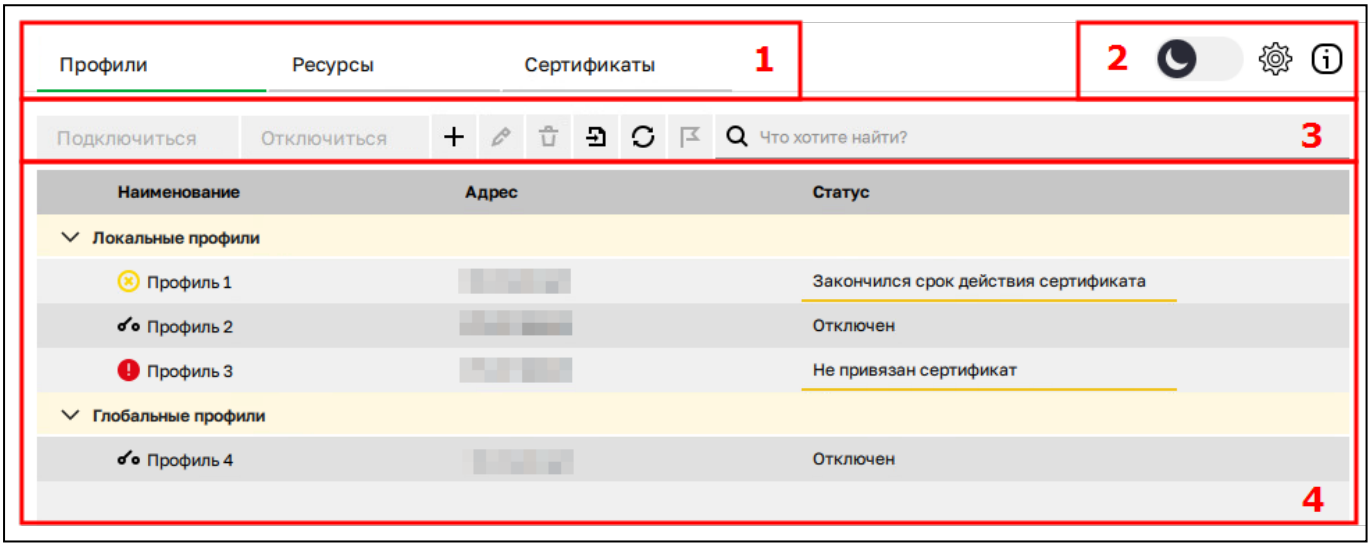
Все события от узлов сети, служб Клиента и любые другие системные события, которые фиксируются и хранятся в журнале, должны удовлетворять минимальным требованиям к хранению в нем.

Информация о событиях может быть просмотрена пользователем.

В случае необходимости с помощью утилиты "Сбор диагностической информации – Континент ZTN Клиент", входящей в дистрибутив Клиента, может быть создан архив с диагностической информацией о работе ПО.

Пользовательский интерфейс основного окна

Для управления Клиентом реализовано специализированное ПО с графическим пользовательским интерфейсом, устанавливаемое на компьютер пользователя.



Основное окно Клиента содержит элементы, приведенные ниже.

Обозначение	Описание
1	Вкладки для навигации по разделам основного окна
2	Кнопки переключения внешнего вида, "Настройки" и "О программе"
3	Панель инструментов и строка поиска
4	Область отображения информации

Глава 2
Установка, регистрация и удаление ПО Клиента

Установка

В ходе установки Клиента будет установлено ПО криптопровайдера "Код Безопасности CSP". Если планируется использовать изделие совместно с криптопровайдером другой фирмы-производителя, установку стороннего ПО необходимо выполнить перед установкой Клиента.

Установка Клиента осуществляется одним из следующих способов:

- с помощью графического инсталлятора (см. ниже);
- с помощью командной строки (см. стр. **12**).

Внимание!
Перед установкой ПО "Континент ZTN Клиент" необходимо удалить ПО "TLS-Клиент" и "Континент-АП".

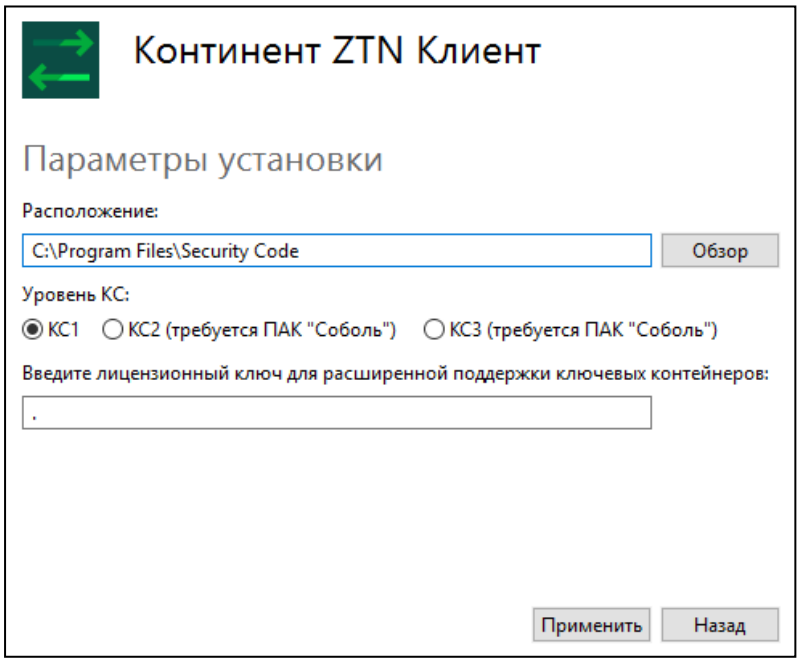
Установка Клиента с помощью графического инсталлятора

Для установки Клиента:

1. Поместите установочный компакт-диск в привод DVD/CD-ROM и затем запустите файл "Континент ZTN Клиент.exe".

   На экране появится окно мастера установки Клиента с текстом лицензионного соглашения.

2. При необходимости указать каталог установки файлов программы, отличный от выбора по умолчанию, уровень КС или ввести лицензионный ключ для расширенной поддержки ключевых контейнеров выполните следующие действия:
   - нажмите кнопку "Настройки" и укажите требуемые значения для соответствующих параметров;
   - нажмите кнопку "Применить" для сохранения указанных данных и возврата в предыдущее окно.



3. Прочитайте лицензионное соглашение и, если вы принимаете его условия, установите отметку в поле "Я принимаю условия лицензионного соглашения", а затем нажмите кнопку "Установить".

   Примечание.
   При появлении окна системы безопасности ОС Windows о подтверждении установки ПО нажмите кнопку "Да" или "Установить".

   Мастер установки выполнит диагностику системы и начнет установку ПО. После успешного завершения установки на экране появится сообщение о необходимости перезагрузки компьютера.

4. Нажмите кнопку "Перезагрузить".

Начнется перезагрузка компьютера. После установки Клиента на рабочем столе ОС Windows появится значок запуска графического приложения "Континент ZTN Клиент", а в меню "Пуск" — раздел "Код Безопасности". В случае установки ПО Клиента в режиме КС1 на экране появится окно набора энтропии.

5. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

   На экране появится окно с сообщением о необходимости регистрации ПО (см. стр. **13**).

Установка Клиента с помощью командной строки

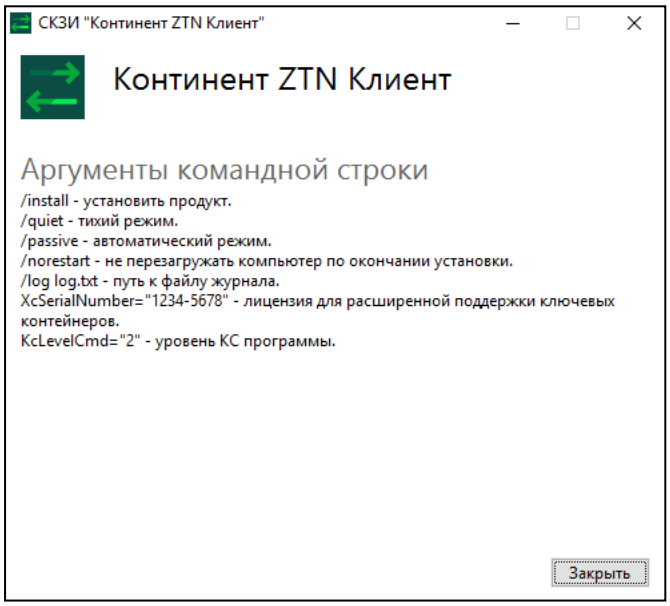
Установка Клиента с помощью командной строки может быть выполнена в следующих режимах — стандартный и тихий. В тихом режиме установка Клиента выполняется без участия пользователя.

Для вызова справки со списком аргументов командной строки для Клиента:

1. Запустите командную строку и перейдите в папку, где находится файл "Континент ZTN Клиент.exe".
2. Выполните следующую команду:

```
"Континент ZTN Клиент.exe" -h
```

   На экране появится список аргументов командной строки для Клиента.



Примечание.
Пример использования указанных на рисунке аргументов см. ниже.

Для установки Клиента в стандартном режиме:

1. Запустите командную строку и перейдите в папку, где находится файл "Континент ZTN Клиент.exe".
2. Выполните следующую команду:

```
"Континент ZTN Клиент.exe" /install
```

   На экране появится окно установки Клиента с текстом лицензионного соглашения.
3. Выполните действия, описанные в шагах **2-5** (см. стр. **11**).

Для установки Клиента в тихом режиме:

1. Запустите командную строку и перейдите в папку, где находится файл "Континент ZTN Клиент.exe".
2. Выполните следующую команду:

```
"Континент ZTN Клиент.exe" /quiet
```

Примечание.
При появлении окна системы безопасности ОС Windows о подтверждении установки ПО нажмите кнопку "Да" или "Установить".

Начнется процесс установки Клиента, после которого компьютер будет перезагружен. После установки Клиента на рабочем столе ОС Windows появится значок запуска графического приложения "Континент ZTN Клиент", а в меню "Пуск" — раздел "Код Безопасности". В случае установки ПО Клиента в режиме КС1 на экране появится окно набора энтропии.

3. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

   На экране появится окно с сообщением о необходимости регистрации ПО (см. стр. **13**).

После установки Клиента в разделе "Код Безопасности" станут доступны приложения, приведенные ниже.

Восстановление Код Безопасности CSP
Восстановление или удаление ПО "Код Безопасности CSP"
Восстановление Континент ZTN Клиент
Восстановление или удаление ПО "Континент ZTN Клиент"
Код Безопасности CSP
Запуск ПО "Код Безопасности CSP"
Континент ZTN Клиент
Запуск ПО "Континент ZTN Клиент"
Контроль целостности – Континент ZTN Клиент
Контроль целостности дистрибутива и установленного на компьютере ПО "Континент ZTN Клиент"
Регистрация – Континент ZTN Клиент
Регистрация ПО на сервере регистрации компании "Код Безопасности"
Сбор диагностической информации – Континент ZTN Клиент
Экспорт отчета о состоянии работоспособности ПО "Континент ZTN Клиент"

Установка стороннего и дополнительного ПО

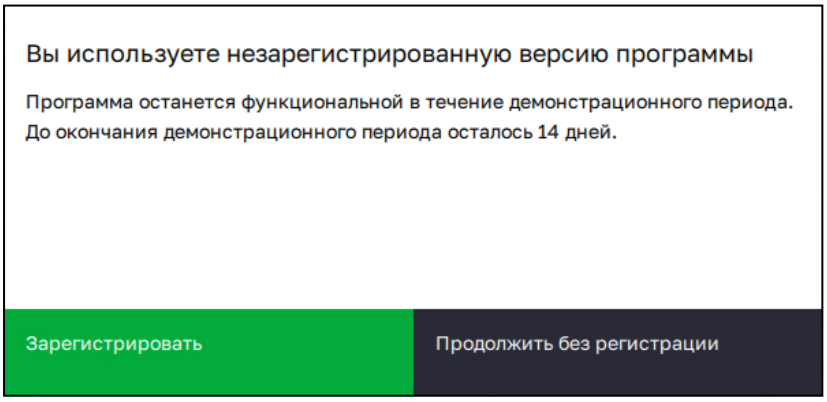
Внимание!

Континент ZTN Клиент необходимо отключать во время установки стороннего ПО, особенно работающего с сетевыми драйверами и интерфейсами (например, Wireshark).

Если предполагается использовать Континент ZTN Клиент с персональными ключевыми носителями, выполните установку соответствующего дополнительного программного обеспечения.

Регистрация

Сразу после установки Клиента начинается демонстрационный период, который составляет 14 дней.



Количество дней до окончания демонстрационного периода отображается в окне "О программе".

Примечание.

Функции Клиента в демонстрационном периоде не ограничиваются.

Если в течение демонстрационного периода регистрация не будет выполнена, при каждом запуске Клиента на экране будет появляться окно с сообщением о необходимости регистрации ПО. При отказе от регистрации по истечении демонстрационного периода работа Клиента будет невозможна до момента успешной регистрации.

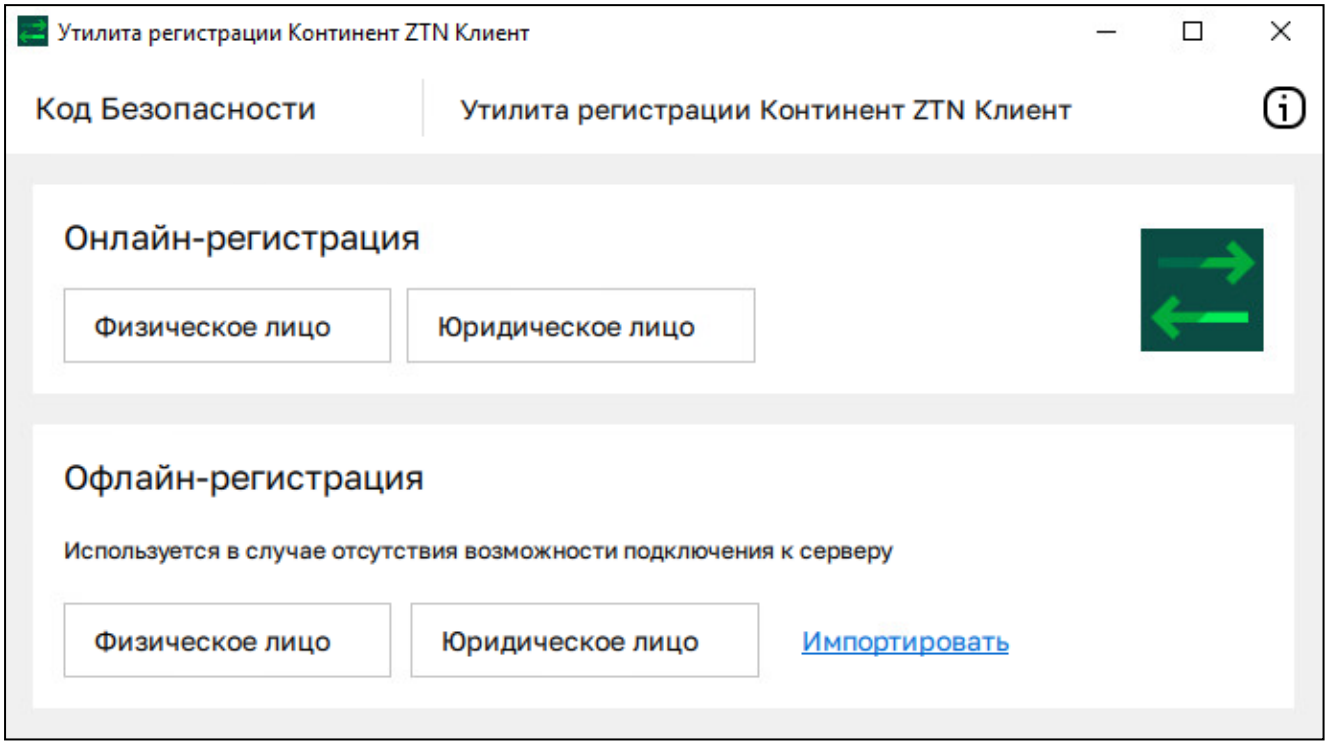
Окно регистрации Клиента можно вызвать вручную, выбрав в меню "Пуск" пункт "Все приложения | Код Безопасности | Регистрация – Континент ZTN Клиент".

Континент ZTN Клиент можно зарегистрировать, выполнив онлайн- или офлайн-регистрацию.

Для онлайн-регистрации:

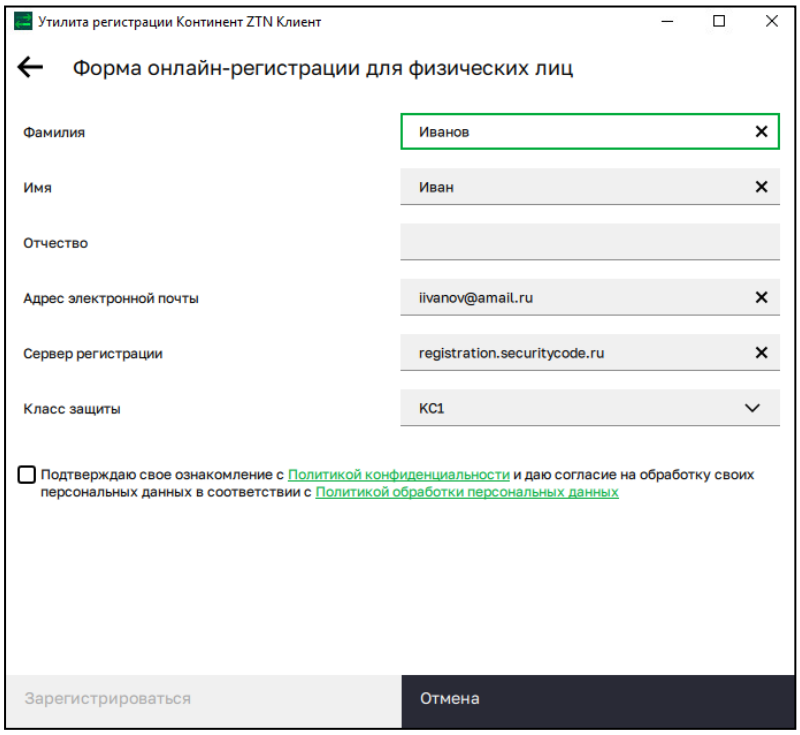
1. В окне сообщения о необходимости регистрации нажмите кнопку "Зарегистрировать".

   На экране появится окно регистрации Клиента.



2. В области "Онлайн-регистрация" нажмите требуемую кнопку — "Физическое лицо" или "Юридическое лицо".

   На экране появится соответствующее окно с формой регистрации.



3. Заполните требуемые поля и нажмите кнопку "Зарегистрироваться".

   Начнется процесс регистрации и подключения к указанному серверу. При его успешном завершении на экране появится соответствующее информационное окно.

Для офлайн-регистрации:

1. В окне регистрации Клиента в области "Офлайн- регистрация" нажмите требуемую кнопку — "Физическое лицо" или "Юридическое лицо".

   На экране появится окно с формой регистрации аналогично онлайн-регистрации (см. стр. **14**).

   Примечание.
   Данные, введенные ранее в форме для онлайн-регистрации, будут автоматически указаны в форме для офлайн-регистрации.

2. Заполните требуемые поля и нажмите кнопку "Сохранить".

   На экране появится стандартное окно сохранения файла.

3. Сохраните файл запроса на регистрацию и передайте его на сервер регистрации для получения файла с серийным номером.

4. После получения файла с серийным номером откройте окно регистрации Клиента и в области "Офлайн-регистрация" нажмите кнопку "Импортировать".

   На экране появится стандартное окно выбора файла.

5. Укажите требуемый файл и нажмите кнопку "Открыть".

   По завершении процесса регистрации на экране появится соответствующее сообщение.

После успешной регистрации ПО Клиента в разделе "О программе" основного окна появится регистрационный номер программы.

Удаление

Удаление Клиента возможно с помощью:

- средств удаления и изменения программ ОС Windows;

  Примечание.
  При удалении Клиента с помощью средств ОС Windows пользовательские настройки ПО сохраняются на компьютере и могут быть применены в дальнейшем, если Континент ZTN Клиент снова будет установлен на компьютер.

- утилиты восстановления ПО "Континент ZTN Клиент";
- MSI-пакета, находящегося на установочном диске.

  Примечание.
  При удалении Клиента с помощью утилиты восстановления или MSI-пакета доступна опция удаления пользовательских настроек ПО.

Удаление ПО "Континент ZTN Клиент" и "Код Безопасности CSP" выполняется по отдельности в любом порядке.

Восстановление

Для восстановления ПО "Континент ZTN Клиент" или "Код Безопасности CSP":

1. В меню "Пуск" в разделе "Код Безопасности" выберите пункт "Восстановление Континент ZTN Клиент" или "Восстановление Код Безопасности CSP".

   На экране появится окно установки ПО.

2. Нажмите кнопку "Далее".

   На экране появится окно для восстановления и удаления ПО.

3. Выберите вариант "Восстановить" и нажмите кнопку "Далее".

4. В появившемся окне нажмите кнопку "Восстановить".

   Начнется восстановление ПО, по завершении которого на экране появится соответствующее сообщение.

5. Нажмите кнопку "Готово".

   На экране появится сообщение о необходимости перезагрузки системы.

6. Нажмите кнопку "Перезагрузить".

Глава 3
Настройка и эксплуатация

Запуск

Континент ZTN Клиент запускается автоматически после входа в систему при включенном параметре "Открывать Континент ZTN Клиент при запуске системы" (см. стр. **38**).

Для запуска Клиента вручную в меню "Пуск" выберите пункт "Все приложения | Код Безопасности | Континент ZTN Клиент" или дважды нажмите левой кнопкой мыши на значок ПО Клиента на рабочем столе.

По умолчанию Клиент запускается в свернутом виде, а на панели задач отображается значок программы, указывающий на состояние соединения.

Значок	Пояснение
	Отключено (соединение не установлено)
	Имеется внутреннее предупреждение. Возможные причины: • выключена проверка по CRL; • незарегистрированная копия ПО
	Соединение установлено

Вызов контекстного меню значка программы на панели задач позволяет осуществить следующие действия:

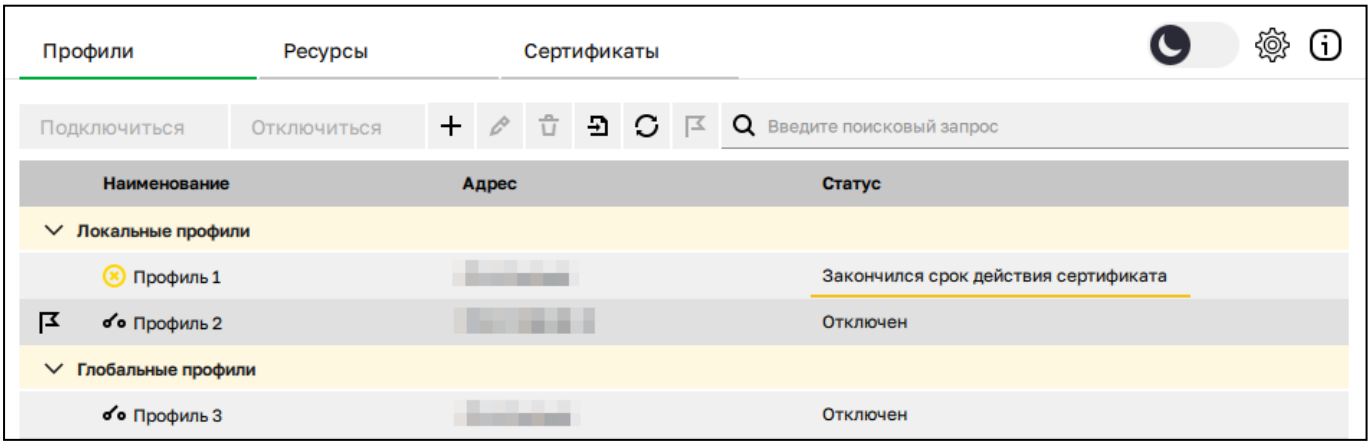
- подключение с профилем по умолчанию или разрыв текущего соединения;
- установление соединения с использованием добавленных профилей или разрыв текущего соединения;
- подключение к избранным ресурсам;
- сброс соединений;
- вызов основного окна ПО (см. стр. **10**);
- завершение работы ПО.

При двойном нажатии левой кнопкой мыши на значок Клиента на панели задач устанавливается или разрывается соединение с СД с использованием профиля по умолчанию.

Управление профилями подключения

Для подключения к СД используются профили подключения, представляющие собой набор настраиваемых параметров. Если к СД должны подключаться несколько зарегистрированных на компьютере пользователей, для каждого из них необходимо добавить отдельный профиль подключения. В списке отображаются только профили пользователя, от имени которого осуществлен вход в систему.

Управление профилями подключения осуществляется в разделе "Профили" основного окна Клиента. Данный раздел содержит список профилей, строку поиска и панель инструментов.



Панель инструментов раздела "Профили" содержит элементы, приведенные ниже.

Кнопка	Описание
Подключиться	Установить соединение с СД, используя профиль, выбранный в списке
Отключиться	Разорвать соединение с СД
+	Добавить профиль
✎	Редактировать параметры профиля
🗑	Удалить профиль
⇥	Импортировать профиль из файла конфигурации
↻	Обновить список профилей
⚑	Использовать профиль для подключения по умолчанию

Создание, настройка и удаление профилей подключения

Континент ZTN Клиент предусматривает использование глобальных и локальных типов профилей.

Перед созданием профиля необходимо подготовить файл сертификата пользователя, полученный от администратора СД, и внешний носитель с ключевым контейнером, если он сохранен на носителе. Файл сертификата можно сохранить на жестком диске или внешнем носителе.

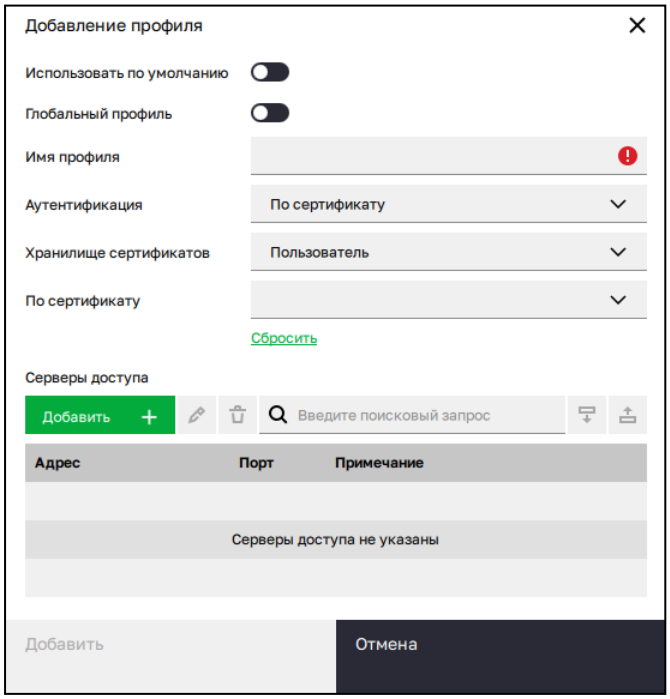
Внимание!

- Для создания и управления глобальными профилями необходимо запустить Клиент от имени администратора.
- Перед созданием глобального профиля убедитесь, что корневой сертификат СД и сертификат пользователя установлены и находятся в хранилище "Локальный компьютер".

Для создания профиля подключения:

1. В основном окне Клиента в разделе "Профили" нажмите кнопку "Добавить" (см. стр. **16**).

   В правой части основного окна появится список настроек профиля подключения.



2. При необходимости установите отметки "Использовать по умолчанию" и "Глобальный профиль".

Примечание.
Подключение с помощью глобального профиля доступно всем пользователям Клиента (см. стр. 22).

3. Укажите имя профиля и выберите в раскрывающемся списке тип аутентификации.
4. В зависимости от типа аутентификации выполните одно из следующих действий:
   - по сертификату — укажите хранилище сертификатов и выберите сертификат пользователя в раскрывающемся списке ниже;

     Примечание.
     При создании глобального профиля хранилище сертификата будет выбрано автоматически.

   - по логину и паролю — введите в открывшиеся поля данные учетной записи пользователя.
5. Для настройки списка адресов СД выполните следующие действия:

Внимание!
Максимальное количество адресов СД для каждого профиля подключения — 10.

   - для добавления адреса СД нажмите кнопку "Добавить". В появившемся окне укажите адрес СД и номер порта, если он должен отличаться от указанного автоматически. Нажмите кнопку "Добавить";
   - для настройки параметров адреса СД выберите адрес и нажмите кнопку "Изменить". В появившемся окне внесите необходимые изменения и нажмите кнопку "Сохранить";
   - для удаления адреса СД выберите адрес и нажмите "Удалить". Подтвердите выполнение операции;
   - для изменения порядка адресов СД выберите адрес и используйте кнопки "Вверх" и "Вниз".
6. Нажмите кнопку "Создать".

   На экране появится уведомление о добавлении профиля. Профиль появится в списке. Для подключения к СД можно использовать только корректно заполненный профиль, имеющий статус "Отключен".

Для редактирования настроек профиля подключения:

Внимание!
Изменять настройки можно только для профиля, не используемого для активного подключения.

1. Выберите профиль и нажмите кнопку "Редактировать" на панели инструментов либо дважды нажмите левой кнопкой мыши по строке профиля.

   В правой части основного окна появится список настроек профиля.
2. Внесите изменения в доступные поля и нажмите кнопку "Сохранить".

Для импорта профиля подключения:

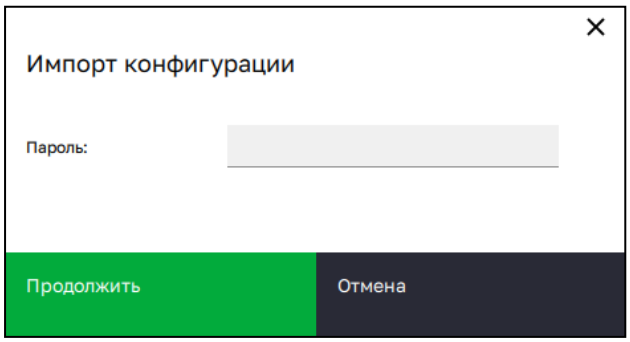
Внимание!
- Поддерживается импорт профилей только для подключения к СД по протоколу версии 4.
- Для импорта конфигурационного файла глобального профиля требуются права администратора.

1. Для импорта профиля нажмите кнопку "Импортировать" на панели инструментов.

Примечание.
Импортируемый ts4-файл может содержать несколько профилей подключения к СД с разными адресами. В таком случае, если хотя бы для одного из импортируемых профилей указан признак глобального профиля, в результате процедуры будет импортирован один глобальный профиль, содержащий все адреса СД, указанные в импортируемом файле.

2. В окне проводника выберите файл конфигурации и нажмите кнопку "Открыть".

   На экране появится окно ввода пароля доступа к файлу конфигурации.



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

   На экране появится окно ввода пароля доступа к ключевому контейнеру.

4. Введите полученный от администратора пароль доступа и нажмите кнопку "ОК".

   На экране появится окно установления нового пароля к ключевому контейнеру.

5. Установите и подтвердите пароль, отличный от предыдущего, а затем нажмите кнопку "ОК".

   Примечание.
   Пароль должен содержать не менее 6 символов, может содержать прописные или строчные буквы латинского алфавита (A–Z, a–z), арабские цифры (0–9) и следующие символы: **? ! : ; " ' , . < > / { } [ ] ~ @ # $ % ^ & * - _ + = \ ` | № ( )**.

   На экране появится окно выбора ключевого носителя для сохранения ключевого контейнера.

6. Выберите ключевой носитель и нажмите кнопку "ОК".

   На экране появится сообщение об успешном выполнении операции.

7. Нажмите кнопку "ОК".

   На экране появится сообщение с предложением произвести пробное подключение с использованием импортированного профиля.

8. Выполните одно из следующих действий:
   - для установления пробного подключения нажмите кнопку "Подключиться";
   - для возврата в раздел "Профили" нажмите кнопку "Закрыть".

   В случае установления подключения на экране появится информационное сообщение.

Для обновления списка профилей нажмите кнопку "Обновить" на панели инструментов.

Для установления профиля по умолчанию выберите профиль и нажмите кнопку "Использовать по умолчанию" на панели инструментов. В строке с профилем появится соответствующий значок.

Автоматическое подключение к СД будет осуществляться по выбранному профилю.

Для отмены данного действия выполните одно из следующих действий:

- нажмите кнопку "Использовать по умолчанию" повторно либо удалите отметку в настройках профиля;
- установите отметку "Использовать по умолчанию" для другого профиля.

Для удаления профиля подключения:

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

1. Выберите профиль и нажмите кнопку "Удалить" на панели инструментов.

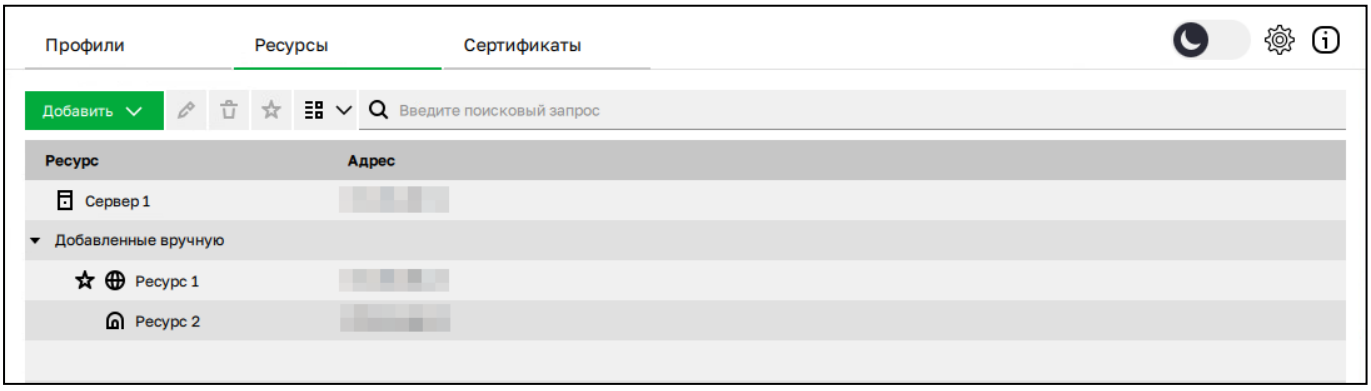
   На экране появится запрос на подтверждение операции.

2. Нажмите кнопку "Удалить".

   Профиль будет удален из списка.

Управление защищенными ресурсами

Управление защищенными ресурсами осуществляется в разделе "Ресурсы" основного окна Клиента. Данный раздел содержит список серверов и ресурсов, строку поиска и панель инструментов.



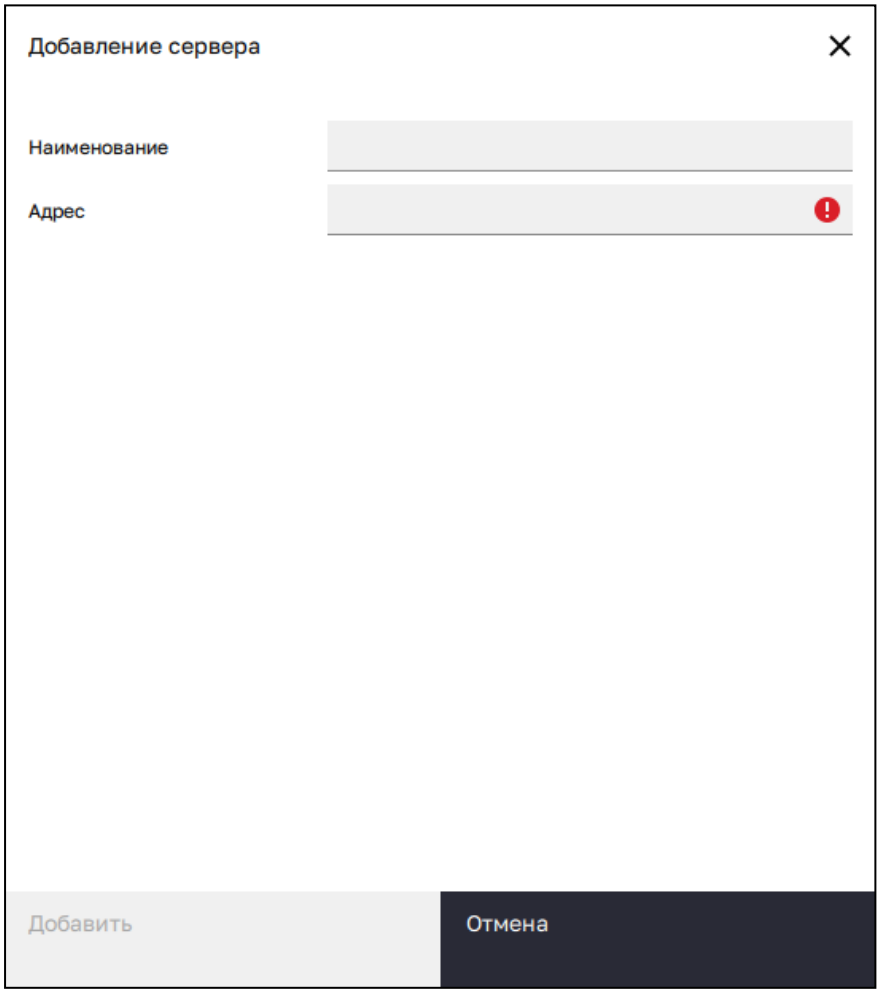
Панель инструментов раздела "Ресурсы" содержит элементы, приведенные ниже.

Кнопка	Описание
Добавить	Добавить сервер/ресурс
	Редактировать параметры сервера/ресурса
	Удалить сервер/ресурс
	Добавить ресурс в избранное
	Режим отображения серверов и ресурсов

Добавление, настройка и удаление защищенных ресурсов

Для добавления сервера:

1. В основном окне Клиента в разделе "Ресурсы" нажмите кнопку "Добавить" на панели инструментов (см. стр. **19**).
2. В раскрывающемся списке нажмите кнопку "Сервер".
   В правой части основного окна появится список настроек сервера.



3. Введите название сервера для установления TLS-подключения в поле "Наименование".
4. Укажите сетевое имя или IP-адрес сервера в поле "Адрес".
5. Нажмите кнопку "Добавить".
   На экране появится сообщение о добавлении сервера.

6. Нажмите кнопку "Закрыть".

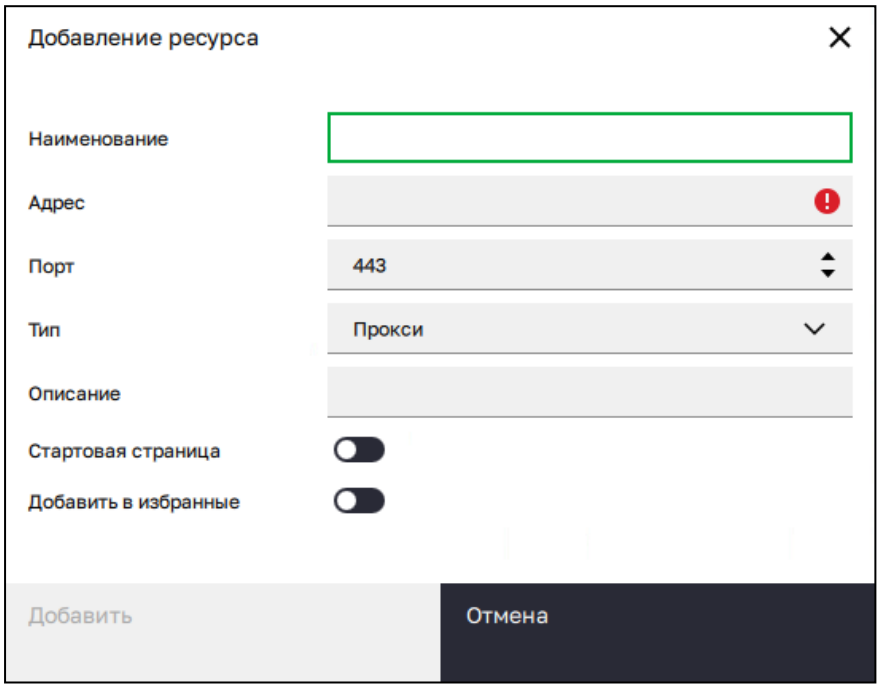
   Сервер появится в списке. На экране появится запрос на загрузку ресурсов.
7. Нажмите кнопку "Да".

   Ресурсы добавленного сервера будут загружены и появятся в списке.

Для создания ресурса:

1. В основном окне Клиента в разделе "Ресурсы" нажмите кнопку "Добавить" на панели инструментов.
2. В раскрывающемся списке нажмите кнопку "Ресурс".

   В правой части основного окна появится список настроек ресурса.



3. Введите название ресурса для установления TLS-подключения в поле "Наименование".
4. Укажите сетевое имя или IP-адрес ресурса в поле "Адрес".
5. Выберите из раскрывающегося списка "Тип" требуемый тип подключения.
6. Установите значение в поле "Порт".
7. При необходимости заполните поле "Описание", а также установите отметки "Стартовая страница" и "Добавить в избранные".

   Примечание.
   Отметки "Начальная страница" и "Избранное" доступны в случае, если в поле "Тип" указано значение "Прокси".
8. Нажмите кнопку "Добавить".

   Ресурс появится в списке.

Для редактирования настроек сервера/ресурса:

Внимание!
Редактирование настроек ресурса, сконфигурированного автоматически, невозможно.

1. Выберите сервер/ресурс и нажмите кнопку "Редактировать" на панели инструментов либо дважды нажмите левой кнопкой мыши по строке требуемого ресурса.

   В правой части основного окна появится список настроек сервера/ресурса.
2. Внесите необходимые изменения в доступные поля и нажмите кнопку "Сохранить".

   На экране появится сообщение об изменении настроек сервера/ресурса.
3. Нажмите кнопку "Закрыть".

   Внесенные изменения будут применены.

Для добавления ресурса в избранное выберите ресурс с типом "Прокси" в списке и нажмите кнопку "Добавить в избранное" на панели инструментов. В строке с ресурсом появится соответствующий значок.

Для отмены действия нажмите кнопку "Добавить в избранное" повторно либо удалите отметку в настройках ресурса.

Для изменения режима отображения перечня серверов/ресурсов нажмите кнопку "Список/дерево" на панели инструментов и выберите в раскрывающемся списке требуемый пункт. Перечень серверов/ресурсов примет необходимый вид.

Примечание.
При переключении на режим отображения "Список" в списке будут отображены только ресурсы.

Для удаления сервера/ресурса:

Внимание!
Удаление ресурса, сконфигурированного автоматически, невозможно.

1. Выберите сервер/ресурс и нажмите кнопку "Удалить" на панели инструментов.
   На экране появится запрос на подтверждение операции.
2. Нажмите кнопку "Удалить".
   Сервер/ресурс будет удален.

Настройка подключения

Перед установлением соединения с СД или защищенными ресурсами необходимо настроить параметры подключения.

Для настройки параметров подключения:

1. В основном окне Клиента нажмите кнопку "Настройки".
   На экране появится окно настройки основных параметров подключения (см. стр. **38**).
2. Настройте значения параметров на требуемых вкладках и нажмите кнопку "Сохранить".
   Внесенные изменения будут применены.

Подключение к серверу доступа

Внимание!
- Подключение к СД возможно только с помощью корректно заполненного профиля, имеющего статус "Отключен".
- Перед подключением к СД необходимо подключить к компьютеру ключевой носитель с закрытым ключом пользователя.

Континент ZTN Клиент позволяет подключиться к СД следующими способами:

- автоматическое подключение после старта Клиента с профилем, назначенным по умолчанию;
- подключение в ручном режиме.

При необходимости можно сохранить пароль для профиля подключения. Для этого требуется установить соответствующую отметку в окне подключения и установить соединение с СД. При следующих подключениях пароль для этого профиля запрашиваться не будет.

Примечание.
- При аутентификации по сертификату сохраняются пароли закрытого ключа и ключевого носителя.
- Если пароль не был сохранен, при установлении соединения с СД в зависимости от типа аутентификации, указанного в настройках профиля, на экране появится окно запроса пароля доступа к ключевому контейнеру или логина и пароля пользователя.

После подключения к СД в строке с используемым профилем значок  станет зеленым.

Автоматическое подключение с профилем по умолчанию

Для настройки подключения:

1. В основном окне Клиента нажмите кнопку "Настройки".
   На экране появится окно настройки основных параметров Клиента.
2. Перейдите на вкладку "VPN".
   На экране появятся настройки режима VPN.
3. Установите отметку "Автоматическое подключение к серверу доступа с профилем по умолчанию".
4. Если при создании или импорте профилей не был назначен профиль по умолчанию, выберите один из списка и установите в его настройках отметку "Использовать по умолчанию" (см. стр. **18**).

При следующем запуске Клиента подключение с данным профилем будет установлено автоматически.

Внимание!

- Если в настройках указано не разрывать соединение при выходе из программы (см. табл. на стр. 40), текущее подключение к СД останется активным в фоновом режиме.
- Автоматическое подключение с профилем по умолчанию не может быть установлено, если пользователь прекратил работу, не разорвав соединение. При попытке подключения на экране появится сообщение: "Автоматическое подключение с профилем по умолчанию не будет производиться, если ранее было установлено другое подключение". Разорвите установленное соединение и перезапустите Континент ZTN Клиент.

Подключение в ручном режиме

Данный способ подключения используется, когда политика безопасности компании запрещает автоматическое подключение к СД.

Для подключения к СД в ручном режиме из панели задач ОС Windows:

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок Клиента в области панели задач и нажмите правую кнопку мыши.
3. Выполните одно из следующих действий:
   - в контекстном меню выберите пункт "Подключиться с "<имя_профиля>";
   - в контекстном меню выберите пункт "Установить соединение", а затем — имя требуемого профиля.

   Начнется процесс подключения с выбранным профилем. При успешном подключении к СД значок на панели задач станет зеленым.

Для подключения к СД в ручном режиме с профилем по умолчанию:

Внимание!

Если при создании или импорте профилей не был назначен профиль по умолчанию, предварительно выберите один профиль из списка и установите в его настройках отметку "Использовать по умолчанию" (см. стр. 18).

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в области панели задач и дважды нажмите левой кнопкой мыши.

   Внимание!

   Подключение устанавливается по первому адресу из списка в выбранном профиле. Если СД, указанный первым, будет недоступен, а количество попыток подключения — исчерпано, начнется установление соединения с СД по следующему адресу в списке.

   Начнется процесс подключения с профилем по умолчанию. При успешном подключении к СД значок на панели задач станет зеленым.

Для подключения к СД в ручном режиме из основного окна Клиента:

1. Запустите Континент ZTN Клиент.
2. В основном окне Клиента выберите раздел "Профили".

   В области отображения информации появится список имеющихся профилей подключения.
3. Выберите профиль и нажмите кнопку "Подключиться" на панели инструментов.

   Если для профиля указано несколько адресов СД, на экране появится окно выбора СД для подключения.
4. Выберите из раскрывающегося списка адрес СД и нажмите кнопку "Подключиться".

   Начнется процесс подключения с выбранным профилем. При успешном подключении к СД значок на панели задач станет зеленым.

Подключение до входа в систему

Подключение к СД/УБ до входа пользователя в систему возможно только с помощью глобального профиля.

Для настройки подключения до входа пользователя в систему:

1. Запустите Континент ZTN Клиент от имени администратора.
2. Выберите пункт "Настройки" на панели навигации и перейдите на вкладку "VPN".

   На экране появятся настройки режима VPN.
3. В области "Режим запуска" установите отметку в поле "Разрешить использование подключения до входа в операционную систему" (см. табл. на стр. 40).

4. Нажмите кнопку "Сохранить".
5. Выполните выход из системы.

   На экране выбора пользователя в правом нижнем углу появится кнопка  ("Вход в сеть").
6. Нажмите кнопку "Вход в сеть".

   На экране появится окно соединения с Клиентом.
7. Выберите в раскрывающемся списке глобальный профиль подключения и нажмите кнопку  .

   Подключение к СД/УБ будет установлено, и на экране появится окно для входа в систему.
8. Для продолжения работы войдите в систему под своей учетной записью.

Разрыв соединения с сервером доступа

Для разрыва соединения с СД из области панели задач дважды нажмите левой кнопкой мыши на значок Клиента или вызовите контекстное меню и нажмите кнопку "Отключить "<имя_профиля>". Соединение с СД будет разорвано, а значок на панели задач станет серым.

Для разрыва соединения с СД из основного окна Клиента:

1. В основном окне Клиента перейдите в раздел "Профили".

   На экране появится список профилей подключения.
2. Выберите профиль, используемый для активного подключения, и нажмите кнопку "Отключиться" на панели инструментов.

   На экране появится окно запроса на подтверждение операции.
3. Нажмите кнопку "Отключить".

   Соединение с СД будет разорвано, а значок на панели задач станет серым. Значок  в строке с профилем, используемым для подключения, станет черным.

Внимание!
- Если после установления соединения с СД выполнена блокировка пользователя ОС, соединение не разрывается.
- При смене пользователя в ОС во время активного подключения, у первого пользователя будет выполнен разрыв соединения.
- При одновременном входе двух и более пользователей в ОС соединение не сможет установить ни один из них.

Доступ к защищенным ресурсам

Для доступа к избранным ресурсам из панели задач ОС Windows:

Примечание.
В список избранных ресурсов могут быть добавлены ресурсы только типа "Прокси".

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в области панели задач и нажмите правую кнопку мыши.
3. В контекстном меню выберите пункт "Избранные ресурсы", а затем — имя требуемого ресурса.

   В веб-браузере откроется страница в соответствии с конфигурацией выбранного ресурса.

Для доступа к защищенному ресурсу с помощью веб-браузера:

1. Запустите веб-браузер и в адресной строке введите адрес ресурса.

   Внимание!
   - При установленном туннеле в веб-браузере необходимо указать протокол, который используется на защищенном веб-сервере.
   - В случае использования сетевого имени ресурса вместо его адреса необходимо осуществить соответствующую настройку DNS-сервера или файла "hosts". После внесения изменений в файл "hosts" требуется перезапустить Клиент.

   Если не установлен сертификат по умолчанию (см. стр. **39**), на экране появится окно выбора сертификата пользователя из списка импортированных сертификатов.
2. Выберите сертификат пользователя и нажмите кнопку "OK".
3. Если на экране появится окно ввода пароля доступа к ключевому контейнеру, введите пароль и нажмите кнопку "OK".

   Окно выбора сертификата закроется, и будет установлено защищенное соединение с указанным ресурсом.

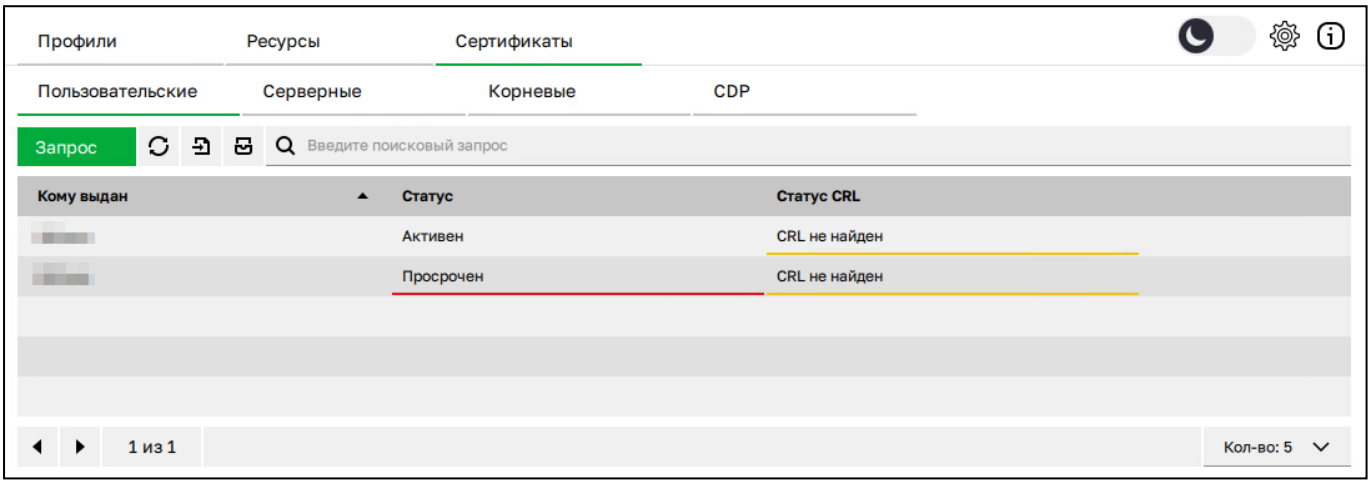
Если пользователь 5 раз подряд в течение 10 минут предъявил недействительный сертификат, доступ к серверу заблокируется на 10 минут (ограничение реализовано на стороне сервера, его параметры могут быть изменены).

Примечание.
Если на TLS-сервере включен режим работы без аутентификации пользователя, для доступа к защищенному ресурсу достаточно запустить веб-браузер и в адресной строке ввести адрес веб-ресурса.

Глава 4
Управление сертификатами

Континент ZTN Клиент позволяет добавлять сертификаты в хранилище, создавать запросы на получение сертификата пользователя и осуществлять запись закрытых ключей на съемный носитель или в Систему (хранилище на локальном компьютере пользователя).

Раздел "Сертификаты" содержит вкладки со списками пользовательских, серверных и корневых сертификатов, CDP, а также строку поиска и панель инструментов.



Панель инструментов раздела "Сертификаты", в зависимости от вкладки, содержит элементы, приведенные ниже.

Кнопка	Описание
Запрос	Создать запрос на сертификат
	Обновить список сертификатов в хранилище/список CDP
	Импортировать сертификат/CRL
	Открыть хранилище сертификатов текущего пользователя
	Удалить сертификат
Добавить +	Добавить CDP вручную
	Редактировать параметры CDP, добавленного вручную
	Удалить CDP, добавленный вручную
	Загрузить CRL из всех добавленных CDP

Для работы с Клиентом необходимы корневые сертификаты, сертификаты пользователя и сервера, получаемые в соответствии с общим порядком, установленным конкретным УЦ. Процедура создания запроса на выдачу сертификата по алгоритму ГОСТ Р 34.10–2012 приводится на стр. **27**.

Примечание.
Допускается использовать действительный уникальный сертификат пользователя, выпущенный УЦ ранее.

Для передачи сертификатов рекомендуется использовать отчуждаемый носитель.

Примечание.
В качестве ключевых носителей могут использоваться USB-флеш-накопители, USB-ключи и смарт-карты (см. стр. 9).

После получения всех сертификатов пользователь должен установить сертификаты в хранилище средствами Клиента (см. стр. **34**), ОС Windows или средствами стороннего криптопровайдера.

Сертификаты	Используемый криптопровайдер	
	Код Безопасности CSP	Сторонний
Корневые	Средствами ОС Windows или Клиента	Средствами ОС Windows или Клиента
Пользовательские	Средствами Клиента	Средствами стороннего криптопровайдера или Клиента (при наличии расширенной поддержки ключевых контейнеров)
Серверные, CDP	Средствами ОС Windows или Клиента	Средствами ОС Windows или Клиента

Для отображения состояния сертификатов используются статусы, приведенные ниже.

Активен
Сертификат действителен
Неактивен
Срок действия сертификата еще не наступил
Просрочен
Срок действия сертификата истек
Срок действия истекает через X дней
Переменная X обозначает количество дней до окончания срока действия сертификата. По умолчанию статус появляется за 14 дней до окончания срока действия сертификата
Не найден корневой сертификат
В пользовательском или серверном сертификате отсутствуют сведения о корневом сертификате
Невозможно построить цепочку сертификатов
Не удалось построить цепочку от пользовательского сертификата до корневого
Нет CRL
Сертификат не прошел проверку по CRL, так как необходимый CRL-файл не импортирован
CRL просрочен
Срок действия CRL истек или еще не наступил
Отозван по CRL
Сертификат не прошел проверку по CRL

Создание запроса на сертификат и закрытого ключа

Запрос на получение сертификата создается пользователем средствами Клиента по требованию администратора безопасности. Одновременно с запросом средствами криптопровайдера генерируется закрытый ключ пользователя.

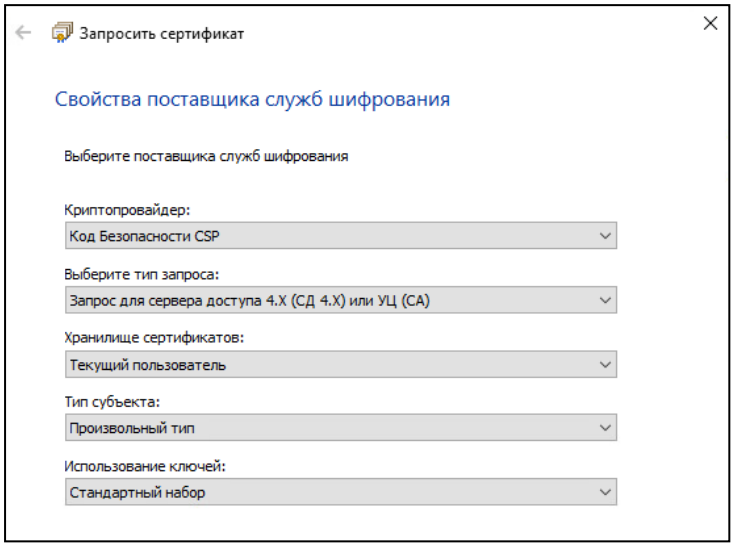
Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе, указанном в настройках.

Примечание.
Рекомендуется заранее подготовить отформатированный ключевой носитель для записи ключевого контейнера.

Для создания запроса на получение сертификата:

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку "Пользовательские сертификаты" и нажмите кнопку "Запрос" на панели инструментов (см. стр. **26**).

   На экране появится окно создания запроса на сертификат.



2. В раскрывающемся списке "Криптопровайдер" выберите требуемое значение.
3. В раскрывающемся списке выберите тип запроса на сертификат.

Запрос для сервера доступа 3.X (СД 3.X)
Для выпуска сертификата в ПУ СД для работы по протоколу версии 3 (алгоритм по ГОСТ Р 34.10-2012)
Запрос для сервера доступа 4.X (СД 4.X) или УЦ (CA)
Для выпуска сертификата в МК (или ПУ СД версий 3.9.1 и 3.9.2 в режиме работы по протоколу версии 4) или внешним центром сертификации (алгоритм по ГОСТ Р 34.10-2012)
Запрос для УЦ КриптоПро
Для дальнейшей обработки в УЦ КриптоПро (алгоритм по ГОСТ Р 34.10-2012)

4. В раскрывающемся списке "Хранилище сертификатов" выберите хранилище ключевого контейнера, в котором будет сохранен закрытый ключ сертификата пользователя:
   - "Текущий пользователь";
   - "Локальный компьютер".

Внимание!
При создании запроса на сертификат, который будет использован в глобальном профиле, необходимо выбрать тип хранилища "Локальный компьютер". Для остальных сертификатов рекомендуется использовать хранилище, предложенное Клиентом по умолчанию.

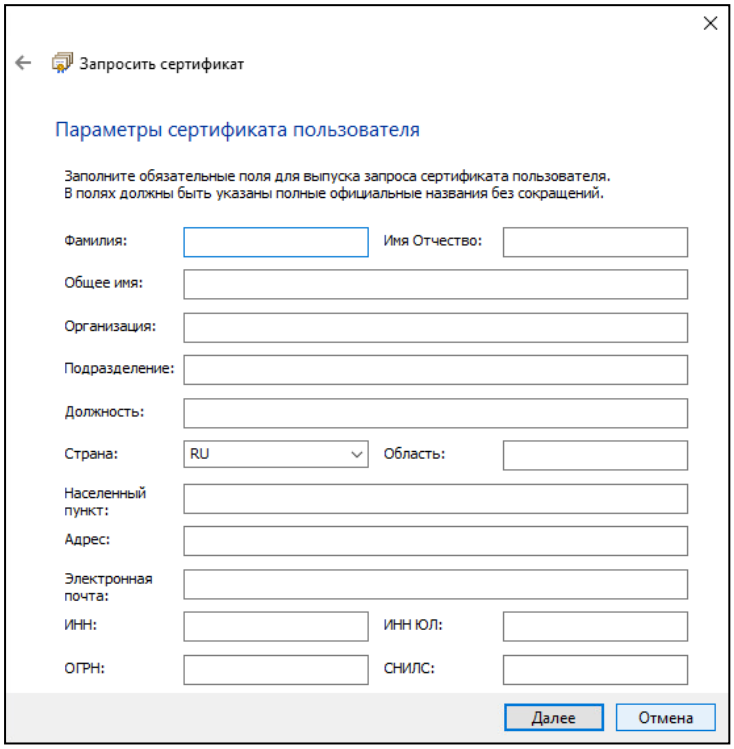
5. В раскрывающемся списке "Тип субъекта" выберите тип пользователя, создающего запрос:
   - "Произвольный тип" (по умолчанию);
   - "Физическое лицо";
   - "Физическое лицо с доверенностью от юридического";
   - "Индивидуальный предприниматель";
   - "Юридическое лицо".
6. В раскрывающемся списке "Использование ключей" укажите набор использования ключей.

Стандартный набор
Минимально необходимые параметры для функционирования ключа шифрования
Расширенный набор
Выбор использования дополнительных параметров ключа шифрования, если это предусмотрено политикой информационной безопасности компании

7. Нажмите кнопку "Далее".

На экране появится диалог для ввода параметров запроса.

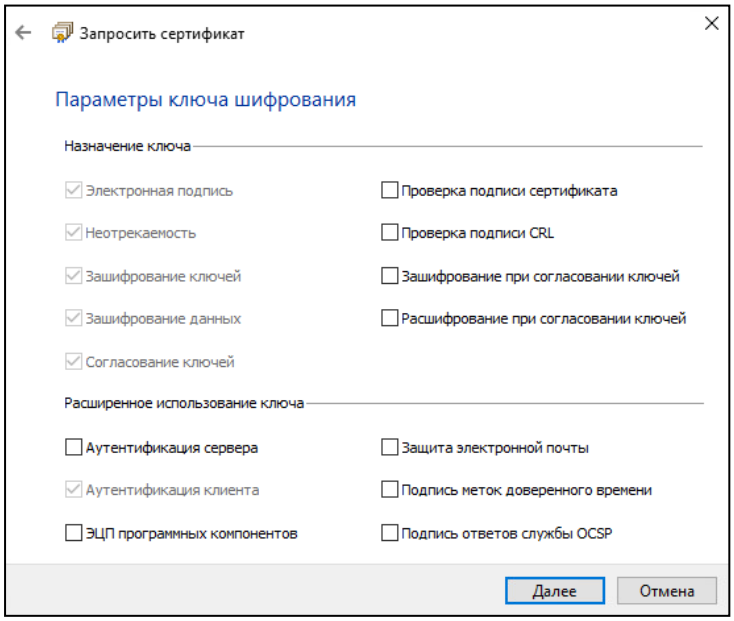
Примечание.
Каждому типу пользователя, создающего запрос, соответствует свой перечень параметров для заполнения. Ниже в качестве примера представлен диалог для ввода параметров запроса произвольного типа пользователя.



8. Заполните требуемые поля и нажмите кнопку "Далее".

Если указан стандартный набор параметров использования ключа, на экране появится окно для ввода дополнительных параметров сертификата. Перейдите к п. **10**.

Если указан расширенный набор параметров использования ключа, на экране появится окно выбора параметров ключа шифрования.

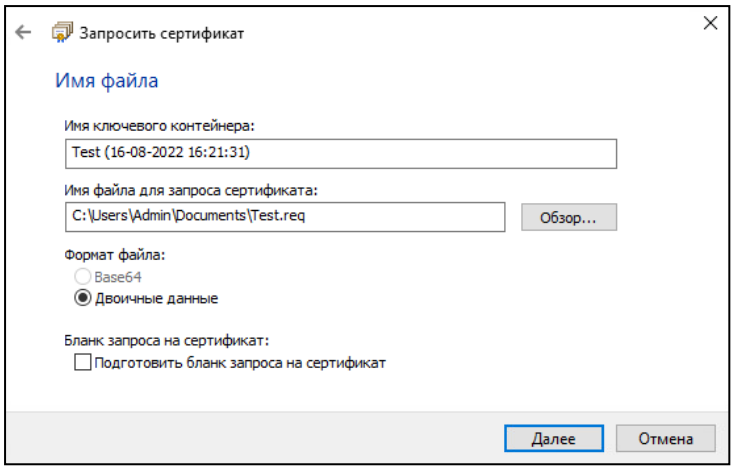


9. Укажите необходимые параметры ключа шифрования и нажмите кнопку "Далее".

На экране появится окно дополнительных параметров сертификата.

10. При необходимости заполните требуемые поля и нажмите кнопку "Далее".

На экране появится окно для определения свойств файла запроса и ключевого носителя.



11. Укажите имя ключевого контейнера и имя файла запроса.

Примечание.
По умолчанию запрос сохраняется в файле с расширением *.req и именем, содержащим имя пользователя, создающего запрос, а также текущие время и дату.

12. Выберите формат, в котором будет сохранен файл запроса.

Внимание!
Для запроса типа "Запрос для сервера доступа 4.X (СД 4.X) или УЦ (CA)" необходимо указать формат файла "Base64".

13. При необходимости установите отметку в поле "Подготовить бланк запроса на сертификат".

Примечание.
Бланк запроса сохраняется в файле с расширением "html" с именем, аналогичным имени файла запроса.

14. Нажмите кнопку "Далее".

На экране отобразятся параметры создаваемого запроса.

15. Нажмите кнопку "Готово".

Начнется процедура создания закрытого ключа.

16. Выполните следующие действия:

Примечание.
Порядок выполнения операций зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации.

- сформируйте закрытый ключ с помощью датчика случайных чисел;

  Примечание.
  Если используется физический датчик случайных чисел ПАК "Соболь", набор энтропии выполняется автоматически и на экране не отображается. Вместо окна накопления энтропии появится окно ввода пароля.

- выберите тип ключевого носителя для записи закрытого ключа;
- введите пароль для ограничения доступа к ключевому контейнеру.

  Примечание.
  - Длина пароля должна быть не менее 6 символов.
  - При наличии отметки в поле "Запомнить пароль" введенный пароль в зашифрованном виде сохраняется в реестре компьютера. Удаление сохраненного пароля возможно с помощью средств "Код Безопасности CSP".

Подробнее о создании закрытого ключа см. на стр. **31**.

Начнется создание запроса и ключевого контейнера. После успешного завершения операции на экране появится соответствующее сообщение.

17. Нажмите кнопку "ОК" и извлеките носитель, если закрытый ключ был сохранен на нем.

18. Передайте созданный файл запроса администратору безопасности. При этом допускается пользоваться общедоступной сетью передачи данных, например, переслать файл как вложение электронной почты.

Варианты использования криптопровайдера при формировании закрытого ключа пользователя

Ниже приведены процедуры формирования закрытого ключа пользователя при создании запроса на получение сертификатов (см. стр. 27) с использованием криптопровайдеров "КриптоПро CSP" и "Код Безопасности CSP".

Внимание!

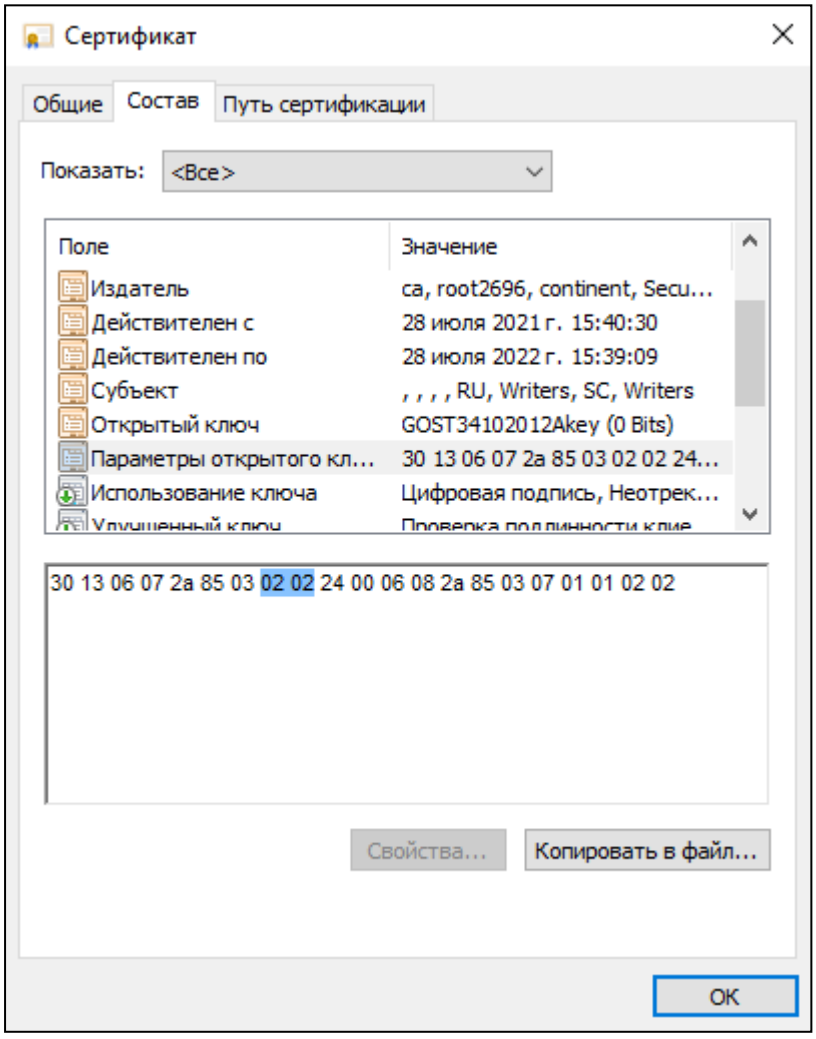
Срок действия закрытого ключа сертификата — 15 месяцев от даты начала срока действия сертификата. По истечении данного периода работа с сертификатом будет невозможна. Необходимо перевыпустить сертификат.

Для проверки валидности сертификата:

1. В основном окне Клиента выберите раздел "Сертификаты".

   В области отображения информации появится список установленных сертификатов.
2. Выберите сертификат, дважды нажав по строке с ним левой кнопкой мыши.

   На экране появится окно просмотра свойства сертификата.
3. Перейдите на вкладку "Состав" и выберите поле "Параметры открытого ключа".
4. Убедитесь, что восьмой и девятый байты слева имеют значение "02", и нажмите кнопку "ОК".

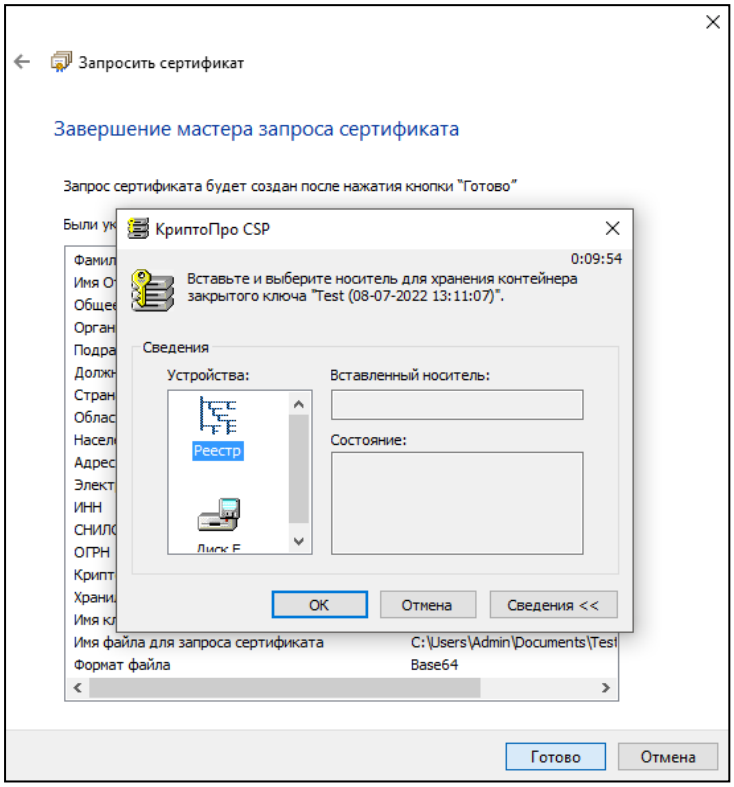


5. В противном случае создайте запрос на другой сертификат или получите новый сертификат из внешних источников.

КриптоПро CSP

Для формирования закрытого ключа:

1. После нажатия кнопки "Готово" в окне завершения работы мастера запроса сертификата на экране появится окно выбора ключевого носителя.



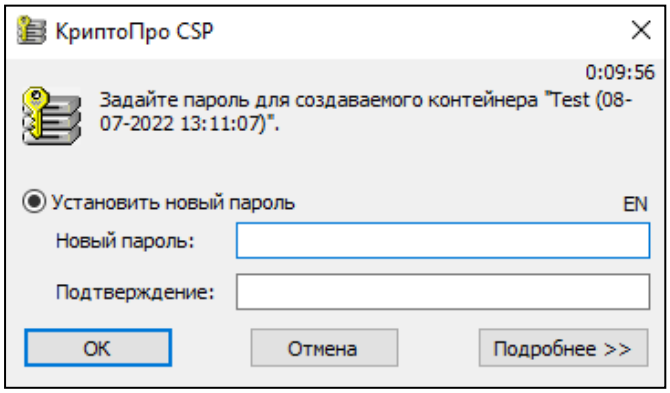
2. Вставьте чистый ключевой носитель и укажите устройство.
3. Нажмите кнопку "OK".

   На экране появится окно "Биологический датчик случайных чисел".

Примечание.
Если в "КриптоПроCSP" настроен датчик случайных чисел ПАК "Соболь", на экране появится окно задания пароля для доступа к содержимому ключевого контейнера. Перейдите к выполнению п. **5**.

4. Следуйте инструкции на экране и дождитесь завершения создания ключа.

   На экране появится окно задания пароля для доступа к содержимому ключевого контейнера.



5. Установите и подтвердите пароль для создаваемого ключевого контейнера и нажмите кнопку "OK".

   Начнется запись закрытого ключа пользователя на ключевой носитель. После ее окончания на экране появится сообщение об успешном создании запроса.
6. Нажмите кнопку "OK".

Код Безопасности CSP

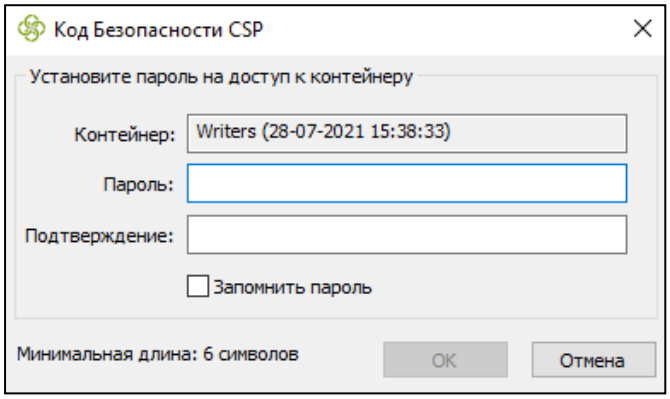
Для формирования закрытого ключа:

1. После нажатия кнопки "Готово" в окне завершения работы мастера запроса сертификата на экране появится окно накопления энтропии для биологического датчика случайных чисел.

   Примечание.
   Если используется физический датчик случайных чисел ПАК "Соболь", набор энтропии выполняется автоматически и на экране не отображается. Вместо окна накопления энтропии появится окно задания пароля. Перейдите к п. **3**.

2. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

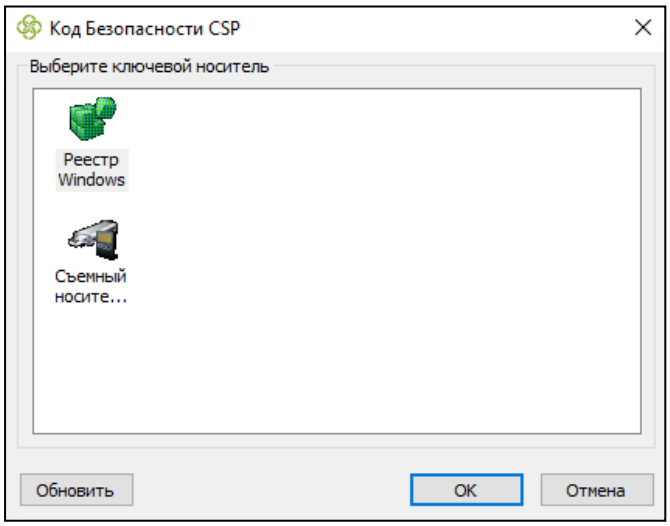
   На экране появится диалог задания пароля для доступа к содержимому ключевого контейнера.



3. Установите и подтвердите пароль для доступа к создаваемому ключевому контейнеру.
4. Нажмите кнопку "OK".

   На экране появится окно выбора ключевого носителя.

   Примечание.
   При необходимости обновить список ключевых носителей нажмите соответствующую кнопку.



5. Выберите требуемый ключевой носитель и нажмите кнопку "OK".

   Начнется создание запроса и криптографического контейнера. После успешного завершения операции на экране появится соответствующее сообщение.
6. Нажмите кнопку "OK" и извлеките носитель.

Импорт и удаление сертификатов

Внимание!
Возможен импорт сертификатов только с использованием алгоритма подписи ГОСТ Р 34.10-2012.

Для импорта пользовательского сертификата:

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку "Пользовательские".

   В области отображения информации появится список установленных сертификатов.
2. Нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится окно настройки параметров импорта сертификата.
3. Нажмите кнопку "Обзор...".

   На экране появится стандартное окно открытия файла.
4. Выберите файл сертификата и нажмите кнопку "Открыть".
5. В окне настройки параметров сертификата нажмите кнопку "Далее".

   На экране появится окно для выбора хранилища сертификатов.
6. В раскрывающемся списке "Хранилище сертификатов" выберите хранилище, в которое будет помещен сертификат.

   Внимание!
   Для сертификатов, которые будут использованы при создании глобальных профилей, необходимо выбрать тип хранилища "Локальный компьютер". Для остальных сертификатов рекомендуется использовать хранилище, предложенное по умолчанию.
7. Для выбора расположения хранилища сертификатов выберите опцию "Поместить все сертификаты в следующую папку", нажмите кнопку "Обзор..." и укажите требуемую папку.
8. Нажмите кнопку "Далее".

   На экране появится окно запроса контейнера закрытого ключа сертификата.
9. Выберите требуемый контейнер и нажмите кнопку "Далее".

   Примечание.
   Для корректного импорта сертификатов с привязкой к ключевому контейнеру пользователю необходимо иметь права, разрешающие запись и/или изменение следующих веток реестра:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY\Keys;
   - HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MY\Keys.

   На экране появится завершающий диалог мастера установки сертификата.
10. Проверьте корректность указанных значений и нажмите кнопку "Готово".

    На экране появится окно ввода пароля доступа к ключевому контейнеру.
11. Введите пароль и нажмите кнопку "ОК".

    Примечание.
    Если при создании запроса на сертификат пароль был сохранен, при импорте данного сертификата пароль запрашиваться не будет.

    Если в папке, в которой хранится пользовательский сертификат, будет обнаружен соответствующий корневой сертификат, на экране появится окно с предложением его импортировать.
12. Нажмите кнопку "Да".

    На экране появится стандартное окно открытия файла.
13. Выберите файл сертификата и нажмите кнопку "Открыть".

    На экране появится сообщение об успешном выполнении операции. Сертификаты появятся в списке.

Для импорта корневого или серверного сертификата:

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку с требуемым типом сертификатов.

   В области отображения информации появится список установленных сертификатов.
2. Нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится окно настройки параметров импорта сертификата.
3. Нажмите кнопку "Обзор...".

На экране появится стандартное окно открытия файла.

4. Выберите файл сертификата и нажмите кнопку "Открыть".

   Корневой или серверный сертификат появится в списке.

Для удаления сертификата пользователя:

Внимание!
Сертификат пользователя не может быть удален, если он привязан к профилю подключения.

1. В основном окне Клиента в разделе "Профили" выберите профиль, к которому привязан сертификат, и нажмите кнопку "Редактировать профиль" на панели инструментов.

   На экране появится список настроек профиля.

2. Выберите другой возможный сертификат пользователя и нажмите кнопку "Сохранить".
3. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "Пользовательские".

   В области отображения информации появится список установленных сертификатов.

4. Выберите сертификат и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится запрос на подтверждение операции.

5. Нажмите кнопку "Удалить".

   Пользовательский сертификат будет удален из списка.

Для удаления корневого или серверного сертификата:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку с требуемым видом сертификата.

   В области отображения информации появится список установленных сертификатов.

2. Выберите сертификат и нажмите кнопку "Удалить".
3. В окне подтверждения нажмите кнопку "Удалить".

   Сертификат будет удален из списка.

Просмотр сведений о сертификатах

Получить сведения об импортированных сертификатах можно с помощью средств Клиента.

Для просмотра сведений о сертификате средствами ОС Windows и Клиента:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку с требуемым типом сертификатов.

   В области отображения информации появится список установленных сертификатов.

2. Нажмите кнопку "Хранилище" на панели инструментов.

   На экране появится окно диспетчера сертификатов.

3. Выберите пункт "ContinentZTNClient | Сертификаты" и дважды нажмите левой кнопкой мыши на требуемый сертификат.

   На экране появится стандартное окно сведений о сертификате.

4. После просмотра сведений закройте диспетчер сертификатов.

Для просмотра сведений о сертификате средствами Клиента:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку с требуемым типом сертификатов.

   В области отображения информации появится список установленных сертификатов.

2. Выберите сертификат в списке и дважды нажмите левой кнопкой мыши по строке с ним.

   На экране появится стандартное окно сведений о сертификате.

3. После просмотра сведений нажмите кнопку "ОК".

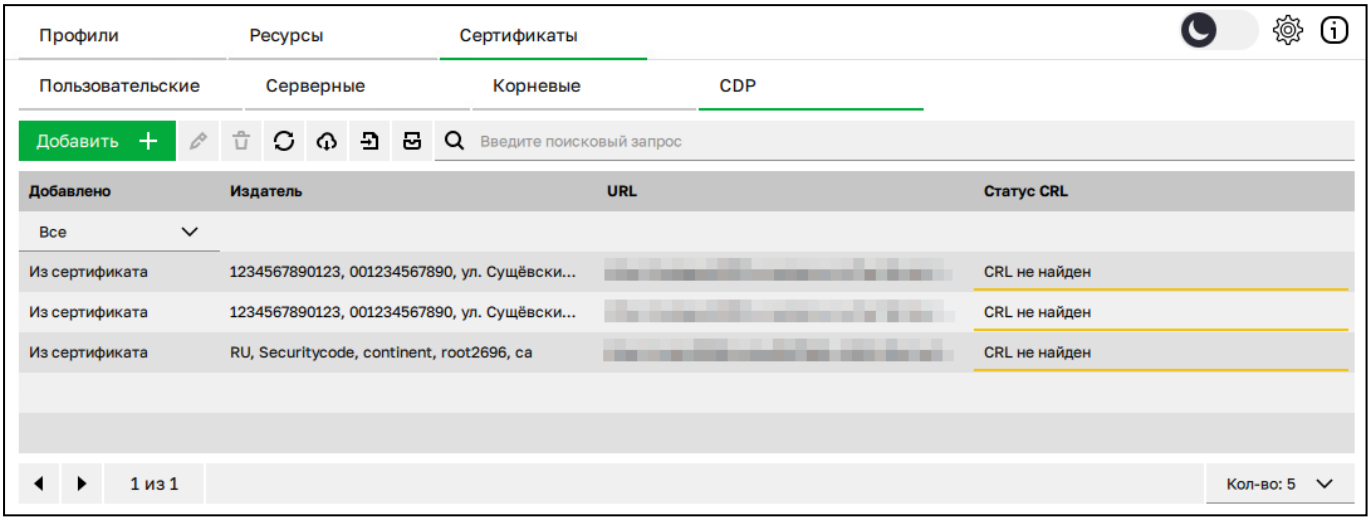
Управление CRL

Континент ZTN Клиент позволяет в автоматическом и ручном режимах получать CDP, а также скачивать CRL для проверки валидности используемых сертификатов.

Управление CRL осуществляется в разделе "Сертификаты" на вкладке "CDP" (см. стр. **26**).

Настройка CDP

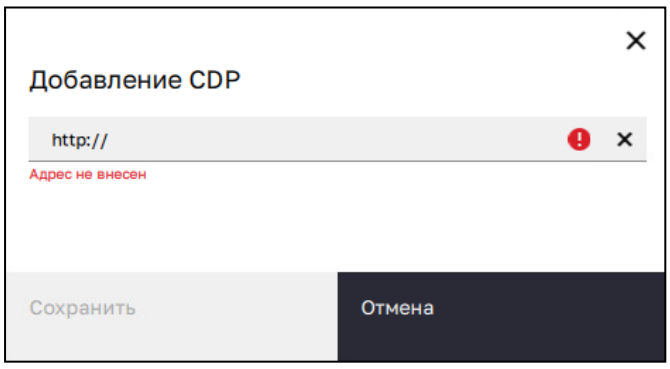
Если используемые сертификаты содержат информацию о CDP, Континент ZTN Клиент получит ее при импорте сертификатов. Для автоматической загрузки CDP необходимо импортировать пользовательский, корневой или серверный сертификат (см. стр. **34**). При необходимости CDP можно добавить вручную.



Примечание.
Для сертификатов, выпущенных в ПУ СД, CRL не требуется. Для подключения к СД отключите проверку CRL в настройках (см. стр. **39**).

Для добавления CDP:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".
   В области отображения информации появится список используемых CDP.
2. Нажмите кнопку "Добавить" на панели инструментов (см. стр. **26**).
   На экране появится окно для ввода адреса CDP.



3. Введите адрес CDP и нажмите кнопку "Сохранить".
   CDP появится в списке.

Для редактирования CDP:

Примечание.
Редактирование CDP, полученного из сертификата, невозможно.

1. В основном окне Клиента на вкладке "CDP" выберите требуемый CDP и нажмите кнопку "Редактировать" на панели инструментов.
   На экране появится окно редактирования CDP.
2. Внесите требуемые изменения и нажмите кнопку "Сохранить".
   Внесенные изменения будут применены.

Для удаления CDP:

Примечание.
Удаление CDP, полученного из сертификата, невозможно.

1. В основном окне Клиента на вкладке "CDP" выберите требуемый CDP и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится запрос на подтверждение операции.
2. Нажмите кнопку "Удалить".

   CDP будет удален из списка.

Для обновления списка CDP нажмите кнопку "Обновить" на панели инструментов.

Примечание.
Редактирование и удаление CDP, полученного из сертификата, невозможно.

Загрузка CRL

Автоматическая загрузка CRL происходит в результате добавления CDP после импорта сертификатов. CRL может быть добавлен вручную с помощью кнопки "Скачать CRL" или с помощью импорта файла.

Если по какой-либо причине CRL не удалось скачать или он был удален, в таблице CDP отобразится соответствующее состояние CRL.

Для обновления списка CRL выполните скачивание CRL вручную.

Для загрузки файлов CRL вручную:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".

   В области отображения информации появится список CDP.

   Примечание.
   Если CDP не прописан в установленном сертификате или не добавлен пользователем ранее, необходимо добавить CDP вручную (см. стр. 36).
2. Нажмите кнопку "Скачать CRL" на панели инструментов.

   Начнется загрузка. После успешного завершения операции на экране появится соответствующее сообщение.
3. Нажмите кнопку "Закрыть".

Для импорта файла CRL:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".

   В области отображения информации появится список имеющихся CDP.
2. Нажмите кнопку "Импортировать CRL".

   На экране появится стандартное окно открытия файла.
3. Укажите загружаемый CRL-файл и нажмите кнопку "Открыть".

   Начнется загрузка. После успешного завершения операции на экране появится соответствующее сообщение.
4. Нажмите кнопку "Закрыть".

Глава 5
Управление работой ПО Клиента

Настройка параметров работы Клиента

Настройка параметров работы Клиента осуществляется в разделе "Настройки" основного окна (см. стр. **10**).

Общие настройки

Для настройки основных параметров Клиента:

Внимание!
Для изменения некоторых основных параметров необходимо запустить Континент ZTN Клиент в режиме администратора.

1. В окне настроек перейдите на вкладку "Общие".
   В области отображения информации появится окно настройки основных параметров подключения.
2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Параметры запуска	
Открывать Континент ZTN Клиент при запуске системы	При включенном параметре ПО Клиента запускается автоматически сразу после загрузки ОС
Свернуть в область уведомлений панели задач	При включенном параметре Клиент запускается в свернутом виде
Подтверждение действий	
Подтверждать сброс соединений	При включенном параметре в случае разрыва соединения по инициативе пользователя на экране появляется окно подтверждения
Настройка работы приложения	
Разрешить управление через консольную утилиту	При включенном параметре возможно осуществлять настройку ПО Клиента с помощью консольной утилиты

3. Нажмите кнопку "Сохранить".

Настройки сертификатов и CRL

Внимание!
Для изменения настроек сертификатов и CRL необходимо запустить Континент ZTN Клиент в режиме администратора.

Для настройки параметров работы с сертификатами и CRL:

1. В окне настроек перейдите на вкладку "Сертификаты".
   На экране появится окно настройки параметров работы с сертификатами и CRL.
2. Установите требуемые значения для параметров в области "Сертификаты пользователя".

Параметр	Описание
Предупреждать об истечении срока действия	Начало периода оповещения пользователя об окончании срока действия сертификата. Принимает значение от 1 до 30 (в днях)
Запрашивать добавление других серверных и корневых сертификатов	При включенном параметре во время первого подключения к СД серверный и корневой сертификаты автоматически добавляются в локальное хранилище компьютера. Для добавления сертификатов в локальное хранилище требуется подтверждение пользователя

3. Установите требуемые значения для параметра в области "Закрытый ключ".

Параметр	Описание
Предупреждать об истечении срока действия	Начало периода оповещения пользователя об окончании срока действия закрытого ключа. Принимает значение от 1 до 30 (в днях)

4. Установите требуемые значения для параметров в области "Параметры CRL".

Параметр	Описание
Проверять подлинность сертификатов	При включенном параметре во время установления соединения с СД и/или TLS-ресурсами осуществляется проверка подлинности сертификатов по CRL
Блокировать работу по истечении срока действия CRL	Период, в течение которого возможно осуществить подключение после истечения срока действия CRL. Принимает значение от 0 до 30 (в днях). Доступно для настройки только при включенном параметре "Проверять подлинность сертификатов"
Автоматическая загрузка CRL	При включенном параметре осуществляется автоматическое обновление CRL с периодичностью, указанной в параметре "Периодичность загрузки CRL"
Периодичность загрузки CRL	Периодичность, с которой осуществляется автоматическая загрузка CRL. Принимает значение от 1 до 48 (в часах). Доступно для настройки только при включенном параметре "Автоматическая загрузка CRL"

5. Нажмите кнопку "Сохранить".

Настройки TLS-соединений

Внимание!

Для изменения некоторых настроек установления TLS-подключения необходимо запустить Континент ZTN Клиент в режиме администратора.

Для настройки параметров работы режима TLS:

1. В окне настроек перейдите на вкладку "TLS".

   В области отображения информации появится окно настройки параметров.

2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Сертификаты пользователя	
Сертификат по умолчанию	Сертификат, который будет автоматически использоваться для подключения к TLS-ресурсам
Сбросить	При нажатии кнопки осуществляется сброс сертификата в поле "Сертификат по умолчанию"
Туннелируемые приложения	
Запускать туннелируемые приложения по ссылкам	При включенном параметре разрешается запуск туннелируемых приложений по ссылке
Уведомлять о запуске приложений	При включенном параметре пользователь получает оповещение, если был осуществлен запуск туннелируемого приложения
Серверные сертификаты	
Проверять подлинность сертификатов	При включенном параметре во время установления соединения с СД и/или TLS-ресурсами осуществляется проверка подлинности сертификатов по CRL
Обновление списка ресурсов	
Проверить наличие обновлений	При нажатии кнопки осуществляется проверка наличия обновлений списка TLS-ресурсов

Параметр	Описание
Автоматически проверять наличие обновлений	При включенном параметре осуществляется автоматическая проверка обновлений списка TLS-ресурсов с периодичностью, указанной в параметре "Периодичность проверки", и временем ожидания, указанным в параметре "Время ожидания соединения"
Периодичность проверки	Период времени (в часах) для автоматического обновления TLS-ресурсов. Принимает значение от 1 до 999. Значение по умолчанию — 1
Время ожидания соединения	Период времени ожидания сервера (в секундах) при обновлении списка TLS-ресурсов. Принимает значение от 1 до 999. Значение по умолчанию — 120
Параметры шифронаборов	
Отключить шифронабор "Магма"	Управление использованием шифронаборов в соответствии с ГОСТ 89, "Магма" и "Кузнечик"
Отключить шифронабор "Кузнечик"	
Отключить шифронабор ГОСТ 89	
Подключение	
Протокол	Используемые версии TLS-протокола для установления соединений. Принимает значения: • TLS v1.0; • TLS v1.2; • TLS v1.0, v1.2
Режим упрощенного подключения	При включенном параметре возможно установление соединения при возникновении проблем с серверным сертификатом

3. Нажмите кнопку "Сохранить".

Настройки режима VPN

Внимание!
Для изменения некоторых параметров режима VPN необходимо запустить Континент ZTN Клиент в режиме администратора.

1. В окне настроек перейдите на вкладку "VPN".

В области отображения информации появится окно настройки параметров режима VPN.

2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Режим запуска	
Автоматическое подключение к серверу доступа с профилем по умолчанию	При включенном параметре устанавливает автоматическое подключение к СД с профилем по умолчанию после запуска Клиента для пользователя, от имени которого осуществлен вход в ОС
Разрешить подключение до входа в систему	При включенном параметре разрешается использовать глобальные профили подключения для установления соединения с СД до входа пользователя в систему
Режим завершения работы	
Разрывать все соединения	При включенном параметре все активные соединения завершаются при завершении работы ПО Клиента. Если параметр выключен, при завершении работы ПО Клиента текущее соединение с СД останется активным в фоновом режиме, а соединения с TLS-ресурсами прервутся
Параметры шифронаборов	
Отключить шифронабор "Магма"	Управление использованием шифронаборов в соответствии с ГОСТ 89, "Магма" и "Кузнечик"
Отключить шифронабор "Кузнечик"	
Отключить шифронабор ГОСТ 89	

Параметр	Описание
Работа приложения	
Блокировать трафик до установления соединения с СД	При включенном параметре вводится запрет на установление незащищенных соединений
Применять новые настройки блокировки трафика при смене СД	При включенном параметре при подключении к другому СД применяются новые настройки блокировки трафика. Доступно для настройки только при включенном параметре "Блокировать трафик до установки соединения с СД"

3. Нажмите кнопку "Сохранить".

Настройки прокси-сервера

Внимание!

Данные настройки прокси-сервера будут использоваться при соединении с СД и защищенными ресурсами, а также при онлайн-регистрации.

Для настройки подключения через внешний прокси-сервер:

1. В окне настроек перейдите на вкладку "Прокси".

В области отображения информации появится окно настройки параметров работы с прокси-сервером.

2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Автоматически определять настройки прокси	При включенном параметре используются системные настройки прокси, а также становятся недоступны отметка "Подключаться через внешний прокси-сервер" и остальные поля для настройки прокси-сервера
Внешний прокси-сервер	
Подключаться через внешний прокси-сервер	При включенном параметре доступна ручная настройка прокси-сервера для установления соединения с СД и TLS-ресурсами
Адрес	Адрес прокси-сервера (URL или IP-адрес)
Порт	Порт прокси-сервера
Исключения	Адреса веб-ресурсов, для подключения к которым не используется внешний прокси-сервер
Аутентификация	
Метод аутентификации	Метод аутентификации на прокси-сервере. Принимает значения: • автоматический выбор; • без аутентификации; • Basic; • NTLM; • Negotiate
Использовать данные текущего пользователя системы (только для режима TLS)	При включенном параметре аутентификация на прокси-сервере осуществляется с использованием учетных данных текущего пользователя ОС
Домен	Домен для аутентификации на прокси-сервере
Учетная запись	Имя учетной записи, принадлежащей указанному выше домену, для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Сбросить сохраненный пароль	При нажатии кнопки осуществляется сброс пароля в соответствующем поле

3. Нажмите кнопку "Сохранить".

Импорт и экспорт конфигурации

На вкладке "Конфигурация" окна "Настройки" осуществляется импорт и экспорт конфигурации Клиента. Конфигурация сохраняется в виде файла с расширением "json".

Для экспорта конфигурации:

1. В окне настроек перейдите на вкладку "Конфигурация".
2. В области "Экспорт" в раскрывающемся списке укажите тип экспортируемых данных:
   - полная конфигурация;
   - профили подключения и настройки;
   - списки ресурсов и настройки;
   - сертификаты.

   Примечание.
   Экспортируемая конфигурация содержит данные о профилях подключения и TLS-ресурсах пользователя, от имени которого осуществлен вход в систему.
3. Нажмите кнопку "Экспортировать".

   При импорте профилей подключения и их настроек или сертификатов на экране появится сообщение о необходимости пользователя самостоятельно произвести экспорт ключевых контейнеров. При импорте списка ресурсов и их настроек на экране появится сообщение о том, что экспорт сертификатов выполнен не будет.
4. Нажмите кнопку "Да".

   На экране появится стандартное окно для сохранения файла.
5. Укажите имя экспортируемого файла и его месторасположение.
6. Нажмите кнопку "Сохранить".

   Файл конфигурации будет сохранен в указанной директории. На экране появятся сообщение об успешном выполнении экспорта и предложение открыть папку расположения файлов конфигурации для дальнейшего импорта настроек.
7. Нажмите кнопку "Да".

   На экране откроется окно соответствующей директории.

Для импорта конфигурации:

1. В окне настроек перейдите на вкладку "Конфигурация".
2. В области "Импорт" нажмите кнопку "Импортировать".

   На экране появится стандартное окно выбора файла.
3. Выберите требуемый файл конфигурации и нажмите кнопку "Открыть".

   При импорте списка ресурсов и их настроек перейдите к п. **6**.

   При импорте профилей подключения и их настроек или сертификатов на экране появится окно обзора ключевых контейнеров.
4. Выберите ключевой контейнер и нажмите кнопку "ОК".

   На экране появится окно ввода пароля доступа к ключевому контейнеру.
5. Введите полученный от администратора пароль доступа к ключевому контейнеру и нажмите кнопку "ОК".

   Выбранная конфигурация будет импортирована. На экране появится соответствующее сообщение.
6. Нажмите кнопку "Закрыть".
7. При необходимости выполните импорт сертификатов вручную (см. стр. **34**).

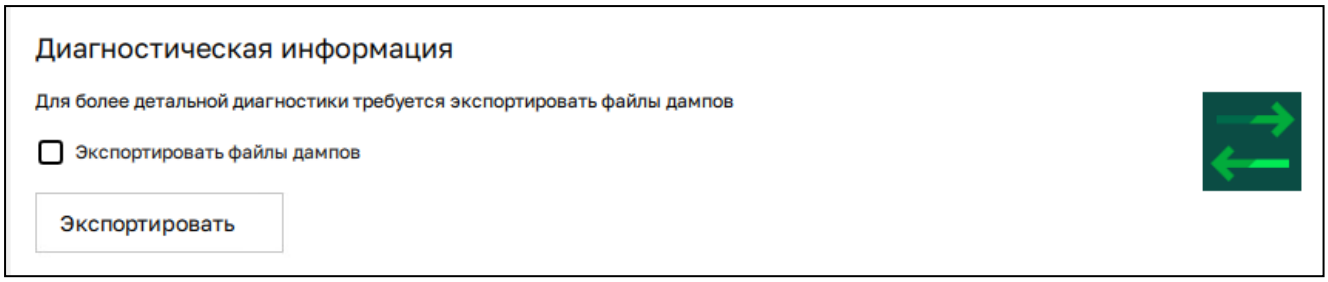
Просмотр событий

События, связанные с работой Клиента, а также установлением соединения с СД и защищенными ресурсами, регистрируются в журнале.

Для сбора диагностической информации:

1. Запустите утилиту "Сбор диагностической информации – Континент ZTN Клиент".

На экране появится окно утилиты сбора диагностической информации.



2. Для включения в сборку файлов дампов установите соответствующую отметку.

Примечание.
При включении файлов дампов в экспортный файл формирование отчета может занять более продолжительное время.

3. Нажмите кнопку "Экспортировать".

   На экране появится стандартное окно сохранения файла.
4. Укажите имя архива и его месторасположение.
5. Нажмите кнопку "Сохранить".

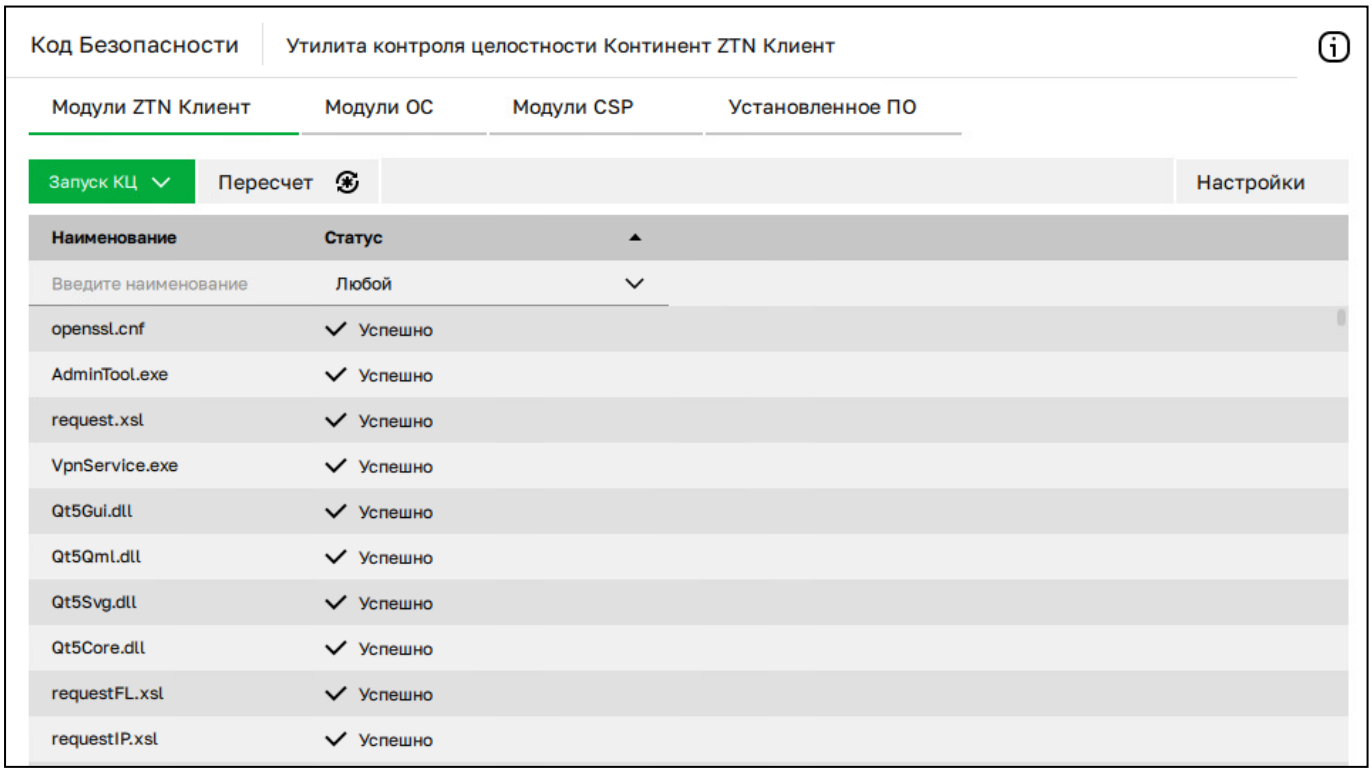
   Архив с диагностической информацией будет сохранен в указанной директории. На экране появится соответствующее сообщение.
6. Нажмите кнопку "Закрыть".

Контроль целостности

Контроль целостности ПО Клиента и файлов ОС, связанных с его функционированием, осуществляется с помощью утилиты "Контроль целостности – Континент ZTN Клиент". При запуске утилиты проверка КЦ начинается автоматически.

Основное окно утилиты содержит следующие вкладки:

- модули Клиента;
- модули ОС;
- модули CSP;
- установленное ПО.



Для проверки целостности вручную:

1. Запустите утилиту "Контроль целостности – Континент ZTN Клиент".

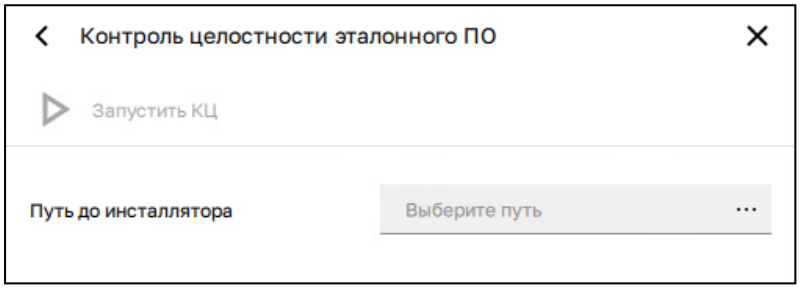
   На экране появится основное окно УКЦ.
2. Перейдите на требуемую вкладку и нажмите кнопку "Запуск КЦ" на панели инструментов.
3. В раскрывающемся списке нажмите кнопку "Программа и операционная система".

   По результатам выполнения операции в соответствующих строках будут обновлены статусы.

Для проверки целостности эталонного ПО:

1. В основном окне УКЦ на вкладке "Модули ZTN Клиента" нажмите кнопку "Запуск КЦ" на панели инструментов.
2. В раскрывающемся списке нажмите кнопку "Эталонное ПО".

   На экране появится окно для запуска процедуры проверки целостности эталонного ПО.



3. В поле "Путь до инсталлятора" укажите месторасположение эталонного ПО.
4. Нажмите кнопку "Запустить КЦ".

   По результатам выполнения операции на экране появится таблица, содержащая названия проверенных файлов, их контрольные суммы и статусы КЦ.
5. Нажмите кнопку "Закрыть".

Для пересчета контрольных сумм:

Примечание.
Для пересчета контрольных сумм требуется запустить УКЦ от имени администратора.

1. В основном окне УКЦ перейдите на требуемую вкладку и нажмите кнопку "Пересчет" на панели инструментов.

   На экране появится запрос на подтверждение операции.
2. Нажмите кнопку "Да".

   По результатам выполнения операции в соответствующих строках будут обновлены статусы.

Для осуществления контроля над установленным ПО:

1. В основном окне УКЦ перейдите на вкладку "Установленное ПО" и установите отметку "Производить контроль установленного программного обеспечения" на панели инструментов.

   Станет доступно выполнение проверки установленного ПО.
2. Установите отметки для ПО, проверку которого необходимо осуществлять.

   Клиент будет осуществлять проверку наличия требуемого ПО на компьютере. По результатам выполнения операции в соответствующих строках будут обновлены статусы.

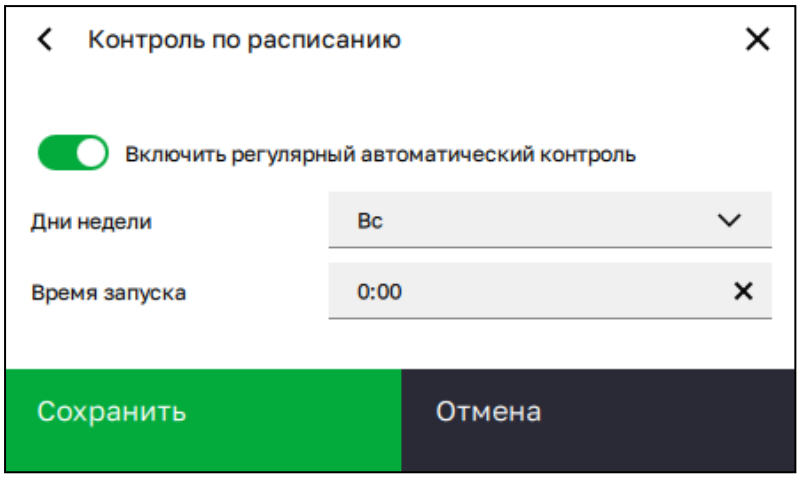
Для настройки проверки целостности по расписанию:

Примечание.
Для настройки расписания необходимо запустить УКЦ от имени администратора.

1. В основном окне УКЦ нажмите кнопку "Настройки" на панели инструментов.

   На экране появится окно с настройками расписания автоматической проверки целостности.
2. Убедитесь, что установлена отметка "Включить регулярный автоматический контроль".

Параметры "Дни недели" и "Время запуска" станут доступными для настройки.



3. В раскрывающемся списке "Дни недели" укажите требуемые значения.
4. В поле "Время запуска" укажите время для начала процедуры проверки целостности по расписанию.
5. Нажмите кнопку "Сохранить".
   Автоматическая проверка целостности будет осуществляться по указанному расписанию.

Приложение

Управление Клиентом через консольную утилиту

Консольная утилита (далее — утилита) позволяет устанавливать соединение Клиента с внешним ПО (API), установленным на том же компьютере. С помощью утилиты имеется возможность устанавливать и разрывать соединение с СД, а также выполнять настройку Клиента.

Для настройки управления Клиентом через утилиту:

Внимание!
Для настройки управления Клиентом через утилиту необходимо запустить Континент ZTN Клиент в режиме администратора.

1. На панели навигации выберите пункт "Настройки".

   В основном окне справа откроется список параметров.
2. Выберите в списке параметров пункт "Общие".

   В области отображения информации откроется соответствующий список настроек.
3. В области "Настройка работы приложения" установите отметку "Разрешить управление через консольную утилиту" (см. табл. на стр. **38**).

   На экране появится окно ввода учетных данных пользователя.
4. Укажите логин и пароль в требуемых полях и нажмите кнопку "Продолжить".
5. В окне "Общие" нажмите кнопку "Сохранить".

   Управление Клиентом через утилиту будет разрешено.

Примечание.
Изменение учетных данных доступно только в приложении Континент ZTN Клиент. Для использования новых учетных данных необходимо выключить, а затем повторно включить параметр "Разрешить управление через консольную утилиту".

Для запрета управления Континент ZTN Клиент через утилиту вернитесь к п. **3**, снимите отметку "Разрешить управление через консольную утилиту" и нажмите кнопку "Сохранить".

Для запуска утилиты:

1. Вызовите командную строку ОС Windows.

   Примечание.
   Для вызова командной строки ОС Windows используйте комбинацию клавиш <Win> и <R>, в появившемся окне введите команду "cmd" и нажмите клавишу <Enter>.
2. Выполните следующую команду:

   ```
   C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe
   ```

   На экране появится перечень параметров, подобный приведенному ниже.

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe
Возможные параметры:
  -? [ --help ]               отображает данное сообщение

  -l [ --login ] arg          задает логин для работы в консольной утилите
                              Использование: -l <login> или --login <login>

  -p [ --password ] arg       задает пароль для работы в консольной утилите
                              Использование: -p <password> or --password
                              <password>

  -v [ --version ]            отображает версию Континент ZTN клиент

  --registrationNumber        отображает регистрационный номер Континент ZTN
                              клиент

  -a [ --about ]              отображает информацию о программе

  --path arg                  задает путь к файлу или папке
                              Использование: --path <path>

  --setProxyConfig            импортирует настройки прокси, используя
                              publicConfig.json
                              Используйте команду вместе с параметром --path
```

Для управления Клиентом через консольную утилиту доступны параметры, приведенные ниже.

Команда	Результат выполнения
-? [--help]	Вывод списка доступных команд
-l [--login] <ЛОГИН>	Ввод логина пользователя
-p [--password] <ПАРОЛЬ>	Ввод пароля пользователя
-v [--version]	Вывод версии Континент ZTN Клиент
--registrationNumber	Вывод регистрационного номера Континент ZTN Клиент
-a [--about]	Вывод информации о программе
--path <ПУТЬ_К_ФАЙЛУ>	Указание пути к файлу
--setProxyConfig	Установка настроек прокси-сервера (необходимо указать путь к файлу "PublicConfig.json")
--exportConfiguration	Экспорт конфигурации (необходимо указать путь для файла конфигурации)
--importConfiguration	Импорт конфигурации (необходимо указать путь к файлу конфигурации)
-c [--connect]	Выполнение подключения с профилем по умолчанию (для выбора другого профиля необходимо указать имя этого профиля)
--disconnect	Разрыв текущего соединения с сервером
--connectionStatus	Вывод текущего состояния подключения
--importServerCertificate	Импорт серверного сертификата (необходимо указать путь к файлу сертификата)
--importRootCertificate	Импорт корневого сертификата (необходимо указать путь к файлу сертификата)
--containerPassword <ПАРОЛЬ_ КОНТЕЙНЕРА>	Ввод пароля доступа к ключевому контейнеру
--profile <ПРОФИЛЬ>	Ввод имени профиля подключения
--setUITheme <ТЕМА>	Выбор темы оформления для Континент ZTN Клиент (необходимо указать значение "light-theme" для выбора светлой темы, "dark-theme" — для темной)
--setRegistrationNumber <НОМЕР>	Ввод регистрационного номера для Континент ZTN Клиент
--offlineRegistration	Выполнение офлайн-регистрации (необходимо указать путь к полученному ранее файлу регистрации)
--addCdp <URL-АДРЕС>	Добавление CDP
--editCdp <СТАРЫЙ URL-АДРЕС> <НОВЫЙ URL-АДРЕС>	Изменение существующего CDP
--removeCdp <URL-АДРЕС>	Удаление CDP
--listCdps	Вывод списка существующих CDP
--importCrl	Импорт CRL (необходимо указать путь к файлу с CRL)
--downloadCrl	Загрузка CRL
--kcLevel	Вывод уровня класса защиты (КС)
--defaultProfileName	Вывод имени профиля по умолчанию
--removeProfile <ПРОФИЛЬ>	Удаление профиля
--addProfile	Добавление профиля (необходимо указать путь к файлу с профилем)
--editProfile	Редактирование профиля (необходимо указать путь к файлу с профилем)
-g [--global]	Параметр для работы с глобальными профилями (требуются права администратора)
--default	Параметр для работы с профилем по умолчанию
--recalculateChecksums	Выполнение процедуры пересчета контрольных сумм
-- disableConsole	Отключение возможности управления Континент ZTN Клиент через утилиту (требуются права администратора)

Команда	Результат выполнения
--disableGui	Отключение возможности управления Континент ZTN Клиент через графический интерфейс (требуются права администратора)
--enableGui	Включение возможности управления Континент ZTN Клиент через графический интерфейс (требуются права администратора)

Примеры команд

Подключение с профилем по умолчанию

Команда осуществляет подключение с профилем по умолчанию:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> -c
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

Подключение по профилю с вводом пароля для доступа к ключевому контейнеру

Команда осуществляет подключение по выбранному профилю:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> -c --profile <ПРОФИЛЬ> --containerPassword <ПАРОЛЬ_КОНТЕЙНЕРА>
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

<**ПРОФИЛЬ**> — имя профиля для подключения.

<**ПАРОЛЬ_КОНТЕЙНЕРА**> — пароль доступа к ключевому контейнеру.

Подключение с глобальным профилем

Примечание.
Для подключения с помощью глобального профиля необходимо запустить командную строку от имени администратора.

Команда осуществляет подключение с глобальным профилем:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> -c -g --profile <ПРОФИЛЬ>
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

<**ПРОФИЛЬ**> — имя глобального профиля для подключения.

Разрыв соединения

Команда осуществляет разрыв текущего соединения:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> --disconnect
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

Настройка подключения через прокси-сервер

Команда осуществляет применение настроек прокси-сервера:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> --setProxyConfig --path <C:\PublicConfig.json>
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

<**C:\PublicConfig.json**> — путь к файлу настроек прокси "PublicConfig.json".

Подключение через прокси-сервер

Команда осуществляет подключение через прокси-сервер:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> -c --profile <ПРОФИЛЬ>
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

<**ПРОФИЛЬ**> — имя профиля для подключения через прокси-сервер.

Отключение графического интерфейса Клиента

Команда осуществляет отключение графического интерфейса Клиента:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> --disableGui
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

После выполнения команды "--disableGui" графический интерфейс Клиента становится недоступен. При попытке запуска программы через графический интерфейс на экране появится соответствующая ошибка.

Включение графического интерфейса Клиента

Команда осуществляет включение графического интерфейса Клиента:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe -l <ЛОГИН>
-p <ПАРОЛЬ> --enableGui
```

<**ЛОГИН**> и <**ПАРОЛЬ**> — учетные данные, введенные в п. **4** (подробнее см. на стр. **46**).

Добавление профиля подключения

Команда осуществляет добавление профиля для подключения к СД:

```
C:\Program Files\Security Code\Continent ZTN Client>ZtnClientConsole.exe
--addProfile --path <JSON>
```

<**JSON**> — путь до json-файла, который содержит сведения о профиле подключения.

Структура и содержание json-файла со сведениями о профиле подключения приводятся ниже.

```
"accessServerAuth": "",
	"certificateSerial": "",
	"certificateSubject": "",
	"connections": [
		{
			"host": "",
			"note": "",
			"tcpPort": ,
			"udpPort":
		}
	],
	"id": ,
	"isLocalMachine": ,
	"login": "",
	"name": "",
	"password": "",
	"passwordEncrypted":,
	"profileType": "",
	"protocol": "",
	"status": ""
```

Допустимые значения параметров профиля подключения, которые указываются в json-файле, приводятся в таблице ниже.

Параметр	Описание
accessServerAuth	Тип аутентификации. Принимает следующие значения: • Certificate — для аутентификации по сертификату; • Password — для аутентификации по логину и паролю
certificateSerial	Серийный номер сертификата
certificateSubject	Имя сертификата
host	Адрес сервера доступа
note	Примечание

Параметр	Описание
tcpPort	Номер TCP-порта
udpPort	Номер UDP-порта
id	ID профиля. Назначается Клиентом автоматически
isLocalMachine	Тип хранилища сертификтов. Принимает следующие значения: • true — хранилище локальной машины; • false — хранилище пользователя
login	Логин для аутентификации по логину и паролю
name	Имя профиля
password	Пароля для аутентификации по логину и паролю
passwordEncrypted	Признак зашифрования пароля. Принимает следующие значения: • true — пароль зашифрован; • false — пароль не зашифрован
profileType	Тип профиля. Принимает следующие значения: • local — локальный профиль; • global — глобальный профиль
protocol	Клиент осуществляет соединение с СД по протоколу версии 4. Параметр принимает единственное значение — "CONT40"
status	Состояние (статус) профиля. Определяется Клиентом автоматически

Особенности совместной работы с КриптоПро CSP

Порядок установки и удаления ПО

Внимание!

- Перед началом установки ПО рекомендуется создать точку восстановления ОС встроенными средствами.
- Процедуру восстановления необходимо осуществлять средствами программы "Восстановление Континент ZTN Клиент".

При необходимости совместной работы ПО Клиента и КриптоПро CSP необходимо осуществлять установку ПО в следующем порядке:

1. КриптоПро CSP.
2. Континент ZTN Клиент и криптопровайдер "Код Безопасности CSP".

Примечание.

После установки требуемого ПО необходимо осуществить перезагрузку компьютера.

В случае возникновения проблем после установки рекомендуется осуществить удаление соответствующего ПО и выполнить установку ПО повторно в порядке, приведенном выше.