КОД безопасности

Континент ZTN Клиент для macOS

Руководство по эксплуатации

АМБС.26.20.40.140.007 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

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
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
URL	Uniform Resource Locator
VPN	Virtual Private Network

Введение

Руководство предназначено для пользователей и администраторов изделия "Континент ZTN Клиент для macOS" АМБС.26.20.40.140.007 (далее — Континент ZTN Клиент, Клиент, изделие). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации изделия на базе операционных систем семейства macOS.

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 семейства macOS 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 изделием "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее — TLS-сервер), а также обмен данными с веб-серверами корпоративной сети;
- регистрация событий, связанных с функционированием Клиента;
- контроль целостности ПО Клиента.

Изделие 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 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

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

Элемент	Требование
Операционная система	• macOS Catalina (10.15); • macOS Big Sur (11); • macOS Monterey (12); • macOS Ventura (13)
Процессор, оперативная память	В соответствии с установленной ОС
Жесткий диск (свободное место)	300 Мбайт
Привод	Привод DVD/CD-ROM

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 осуществляется 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 производится 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 осуществляется 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 встроенной криптобиблиотеки.

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 программного обеспечения Клиента (см. стр. **24**). 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;
- путем построения цепочки сертификатов.

Контроль целостности

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

Осуществляется сравнение текущих значений контрольных сумм контролируемых файлов и эталонных значений, рассчитанных в ходе установки Клиента. 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 в следующих случаях:

- при запуске Клиента и УКЦ;
- до установления соединения с СД и защищенными веб-ресурсами;
- вручную, с помощью УКЦ;
- по расписанию, настраиваемому с помощью УКЦ (по умолчанию ежедневно в 12:00 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 Континент ZTN Клиент будет активным, рабочие сессии с защищенными ресурсами продолжатся. Установление соединения с СД и создание новых сессий будет заблокировано.

При обнаружении нарушения целостности при неактивном ПО Клиента будет сделана соответствующая запись в журнале событий.

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

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

Аудит

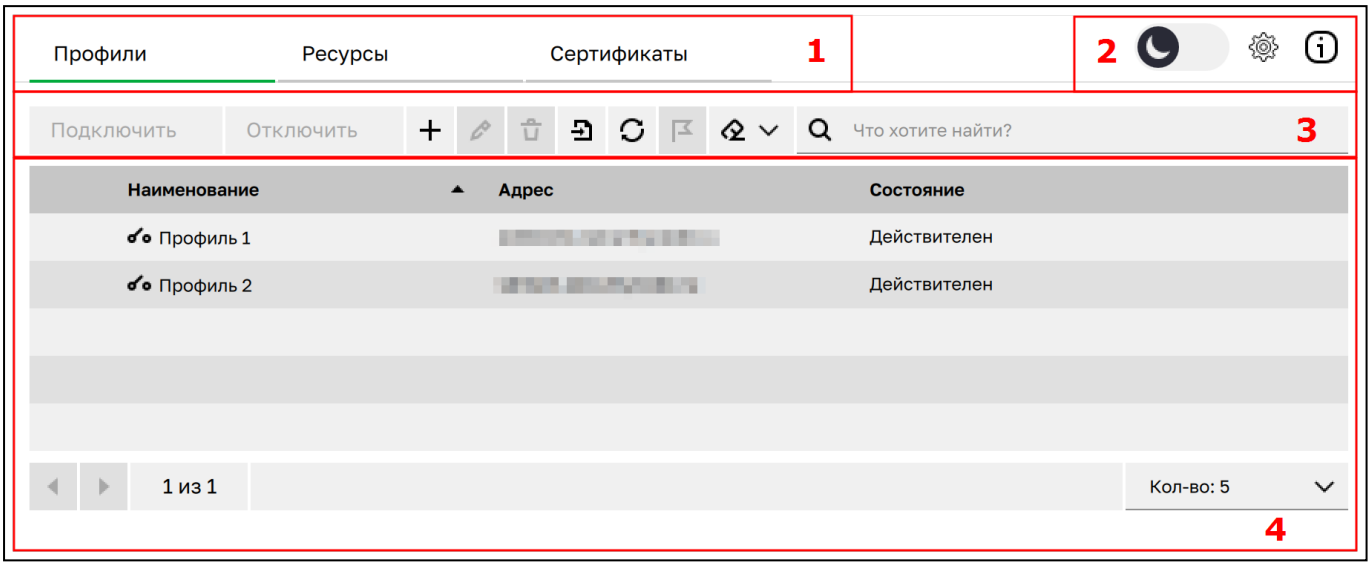
Все события от узлов сети, служб Клиента и любые другие системные события, которые фиксируются и хранятся в журнале, должны удовлетворять минимальным требованиям к хранению в нем.

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 (см. стр. **37**).

Пользовательский интерфейс основного окна

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



Основное окно Континент ZTN Клиент 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 и удаление ПО

Установка

Внимание! Для установки ПО Клиента требуются права администратора.

Для установки программного обеспечения:

1. Перейдите в директорию, содержащую установочный пакет ПО Клиента, и откройте соответствующий файл-образ с расширением "*.dmg".
2. В появившемся окне выберите файл с расширением "*.mpkg", одновременно нажмите левую кнопку мыши и клавишу <control>, в контекстном меню нажмите кнопку "Открыть".
3. В появившемся окне предупреждения нажмите кнопку "Открыть", далее — кнопку "Разрешить".

   На экране появится окно установки ПО Клиента.
4. Нажмите кнопку "Продолжить".

   На экране появится окно с текстом лицензионного соглашения.

   Примечание. При необходимости выберите из раскрывающегося списка требуемый язык.
5. Прочитайте текст соглашения и, если вы с ним согласны, нажмите кнопку "Продолжить".

   Примечание. Для сохранения/печати текста соглашения используйте соответствующие кнопки.

   На экране появится окно запроса на подтверждение операции.
6. Нажмите кнопку "Принять".

   Внимание!
   - Если вы не согласны с лицензионным соглашением, нажмите кнопку "Не принимать". Окно установки ПО Клиента закроется.
   - Для повторного ознакомления с соглашением нажмите кнопку "Прочитать лицензию". Произойдет возврат в предыдущее окно.

   На экране появится окно, содержащее детали установки ПО Клиента.
7. При необходимости выполните следующие действия:
   - если требуется выбрать другой диск для установки Клиента, нажмите кнопку "Изменить размещение установки...", в появившемся списке укажите доступный диск и нажмите кнопку "Продолжить";
   - если необходимо осуществить выборочную установку, нажмите кнопку "Настроить" и в появившемся окне установите отметки для компонентов в требуемое состояние.

     Примечание. Для возврата в предыдущее окно нажмите кнопку "Стандартная установка".
8. Нажмите кнопку "Установить".

   На экране появится окно ввода пароля учетной записи.
9. Введите пароль и нажмите кнопку "Установить ПО".

   На экране появится окно с результатом выполнения установки.
10. Нажмите кнопку "Перезагрузить".

    После перезагрузки устройства откройте меню "Launchpad" и выберите приложение "Континент ZTN Клиент".

    На экране появится окно набора энтропии.
11. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

    После завершения операции в строке меню появится значок Клиента.

    В правой верхней части экрана появится запрос на разрешение уведомлений от Клиента.
12. Нажмите кнопку "Параметры", а затем — кнопку "Разрешить".

Вид значка Клиента указывает на состояние соединения.

Значок	Пояснение
	Отключено (соединение не установлено)
	Имеется внутреннее предупреждение (например, выключена проверка по CRL)
	Соединение установлено (подробнее см. на стр. **33**)

В меню "Launchpad" появятся значки приложений, входящих в состав Клиента.

Станут доступны приложения, приведенные ниже.

Диагностика (Сбор диагностической информации – Континент ZTN Клиент)
Экспорт отчета о состоянии работоспособности ПО Континент ZTN Клиент
Континент ZTN Клиент
Запуск ПО Континент ZTN Клиент
Контроль целостности (Контроль целостности – Континент ZTN Клиент)
Контроль целостности дистрибутива и установленного на компьютере ПО Клиента
Управление ключами (Управление ключевыми контейнерами – Континент ZTN Клиент)
Импорт, копирование, перенос и удаление закрытого ключа, сформированного Клиентом, с внешнего носителя

Удаление

Внимание! Для удаления ПО Клиента требуются права администратора.

Для удаления программного обеспечения:

1. Перейдите в директорию, содержащую установочный пакет ПО Клиента, и откройте соответствующий файл-образ с расширением "*.dmg".
2. В появившемся окне выберите файл "uninstall.tool", одновременно нажмите левую кнопку мыши и клавишу <control>, в контекстном меню нажмите кнопку "Открыть".

   На экране появится окно программы "Терминал" с предложением удалить ПО Клиента.
3. Нажмите клавишу <д> и клавишу <Enter>.

   В окне программы появится запрос ввода пароля администратора.
4. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится запрос на удаление файлов приложения.
5. Выполните одно из следующих действий:
   - для удаления конфигурационных файлов приложения нажмите клавишу <д>;
   - для удаления приложения с сохранением его конфигурационных файлов нажмите клавишу <н>.
6. Нажмите клавишу <Enter>.

   Будет выполнено удаление ПО Клиента. На экране появится запрос на перезагрузку устройства.
7. Нажмите клавишу <д>.

Глава 3
Настройка и эксплуатация

Запуск

Автоматический запуск Клиента после входа в систему по умолчанию выключен (для активации параметра необходимо перейти в настройки и установить соответствующую отметку, см. табл. на стр. **33**). Запуск Клиента вручную осуществляется в меню "Launchpad" или с помощью значка в строке меню (см. стр. **11**).

Клиент по умолчанию запускается в свернутом виде, а в строке меню отображается значок ПО.

Вызов контекстного меню значка ПО Клиента в строке меню позволяет осуществлять 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 Клиента (см. стр. **10**);
- завершение работы ПО.

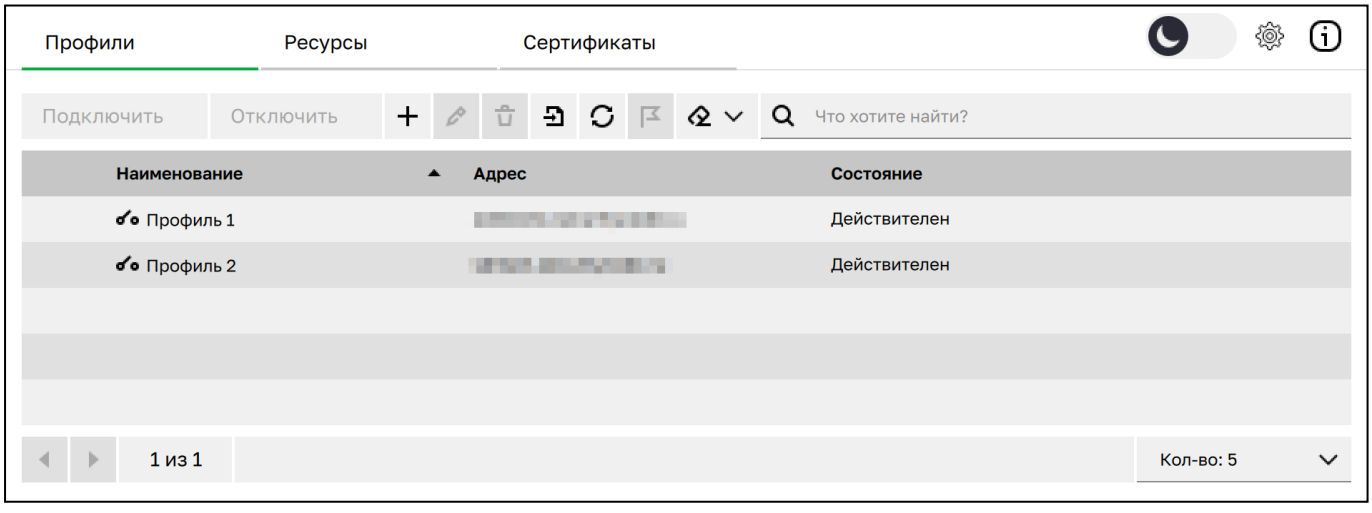
При двойном нажатии левой кнопкой мыши по значку программы в строке меню устанавливается или разрывается соединение с СД с использованием профиля по умолчанию.

Управление профилями подключения

Для подключения к серверам доступа комплекса "Континент" 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 профилей отображаются только профили пользователя, от имени которого осуществлен вход в систему.

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



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

Кнопка	Описание
Подключить	Установить соединение с СД, используя профиль, выбранный в списке
Отключить	Разорвать соединение с СД

Кнопка	Описание
	Добавить профиль
	Редактировать параметры профиля
	Удалить профиль
	Импортировать профиль из файла конфигурации
	Обновить список профилей
	Использовать профиль для подключения по умолчанию
	Удалить сохраненные пароли из профиля либо все пароли

Параметры профиля подключения

Доступные для настройки параметры профиля подключения приводятся ниже.

Использовать по умолчанию
Профиль, с помощью которого соединение с СД после запуска Клиента устанавливается автоматически (если параметр включен, см. стр. **33**) или при двойном нажатии на значок Клиента в строке меню
Наименование
Имя профиля, отображаемое в списке используемых профилей
Тип аутентификации
Тип аутентификации пользователя — по сертификату или паре "логин–пароль"
Сертификат
Имя выбранного сертификата пользователя из списка ранее импортированных сертификатов. Доступно для настройки только при выборе типа аутентификации по сертификату (см. выше)
Сбросить
При нажатии кнопки осуществляется сброс сертификата, выбранного в поле "Сертификат"
Ключевой контейнер
Выбор ключевого контейнера осуществляется с помощью кнопки "Установить" (). При нажатии открывается окно выбора ключевого контейнера. Любая операция с ключевым контейнером требует подтверждения паролем доступа к этому контейнеру. Доступно для настройки только при выборе типа аутентификации по сертификату (см. выше)
Логин/Пароль
Учетные данные пользователя. Доступно для настройки только при выборе типа аутентификации по паре "логин–пароль" (см. выше)
Адреса серверов доступа
Перечень доступных для подключения СД. Панель инструментов, предназначенная для настройки списка адресов СД, становится доступна после добавления первого адреса СД
Адрес
IP-адрес или имя СД. Доступно для настройки при добавлении адреса СД или редактировании его параметров
Порт
Порт СД для установления соединения. Доступно для настройки при добавлении адреса СД или редактировании его параметров

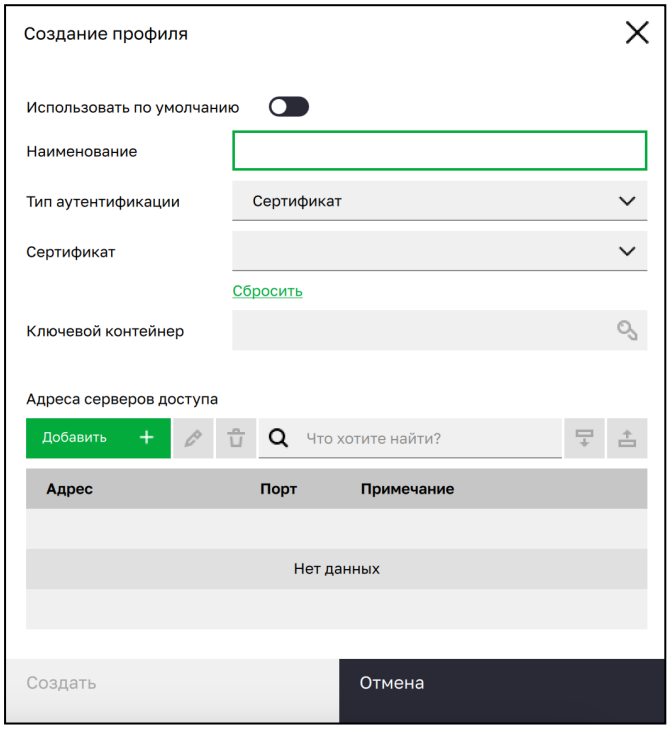
Создание, настройка и удаление профилей подключения

Перед созданием профиля необходимо подготовить файл сертификата пользователя, полученный от администратора СД, и внешний носитель с ключевым контейнером, если ключевой контейнер сохранен на нем, а не в системном хранилище локального компьютера.

Для создания профиля подключения:

1. В основном окне Клиента в разделе "Профили" нажмите кнопку "Добавить профиль" на панели инструментов (см. стр. **13**).

   На экране появится окно "Создание профиля".



Примечание. Если профиль подключения планируется использовать по умолчанию, установите соответствующую отметку.

2. Введите имя профиля в поле "Наименование".
3. В раскрывающемся списке "Тип аутентификации" укажите требуемое значение.
4. В зависимости от указанного типа аутентификации выполните одно из следующих действий:
   - по сертификату — выберите из раскрывающегося списка сертификат пользователя. В поле "Ключевой контейнер" появится имя соответствующего ключевого контейнера;

     Примечание.
     - Для сброса сертификата нажмите соответствующую кнопку.
     - Поле "Ключевой контейнер" заполнится автоматически, если ранее на компьютере (даже для другого профиля) была сохранена пара "Сертификат" – "Ключевой контейнер".
   - по логину и паролю — введите в открывшиеся поля данные учетной записи пользователя.
5. Для настройки списка адресов СД выполните следующие действия:

   Внимание!
   - Соединение с СД устанавливается по первому адресу из списка в выбранном профиле. Если СД, указанный первым, будет недоступен, а количество попыток подключения — исчерпано, начнется установление соединения со следующим адресом СД.
   - Максимальное количество адресов СД для каждого профиля подключения — 50.

   - для добавления адреса СД нажмите кнопку "Добавить". В появившемся окне укажите адрес/имя СД и номер порта, если он должен отличаться от указанного автоматически. Нажмите кнопку "Добавить";

     Примечание.
     - В поле "Адрес" необходимо ввести значение, указанное в поле "CommonName" сертификата сервера.
     - При наличии дополнительных адресов СД в профиле они должны быть представлены DNS-именами. СД, имеющие одинаковые значения в полях "Адрес" и "Порт" или представленные IP-адресами, будут проигнорированы.

- для настройки параметров адреса СД выберите адрес/имя и нажмите кнопку "Изменить". В появившемся окне внесите необходимые изменения и нажмите кнопку "Сохранить";
- для удаления адреса СД выберите адрес/имя и нажмите кнопку "Удалить". Подтвердите выполнение операции;
- для изменения порядка адресов СД выберите адрес/имя и используйте кнопки "Вверх" и "Вниз".

6. Нажмите кнопку "Создать".

   Профиль появится в списке. Для подключения к СД профиль должен иметь статус "Действителен".

Для редактирования настроек профиля подключения:

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

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

   В правой части основного окна появится список настроек профиля.

2. Внесите изменения в доступные поля и нажмите кнопку "Сохранить".

   Изменения будут применены.

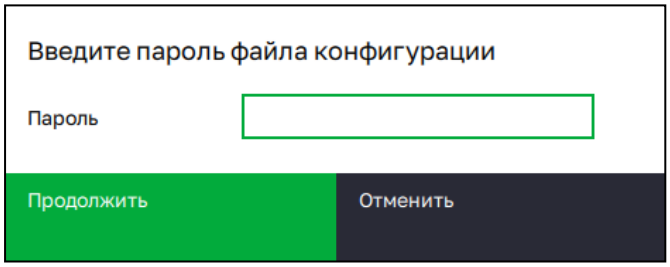
Для импорта профиля подключения:

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

   На экране появится стандартное окно выбора файла.

2. Выберите файл конфигурации и нажмите кнопку "Открыть".

   На экране появится окно ввода пароля доступа к файлу конфигурации.



3. Введите полученный от администратора пароль для файла конфигурации и нажмите "Продолжить".

   Примечание. Максимальное количество попыток ввода пароля доступа к файлу конфигурации — 5. После 5-й неудачной попытки выполнение операции будет прервано.

   На экране появится окно ввода пароля доступа к ключевому контейнеру.

4. Введите полученный от администратора пароль к ключевому контейнеру и нажмите кнопку "ОК".

   Примечание. Максимальное количество попыток ввода пароля доступа к ключевому контейнеру — 5. После 5-й неудачной попытки выполнение операции будет прервано.

   На экране появится окно установления пароля.

5. Введите пароль в требуемых полях и нажмите кнопку "ОК".

   Примечание. Пароль должен содержать не менее 6 символов, прописные и 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 "Выбрать".

   На экране появится окно ввода имени профиля.

7. Укажите наименование профиля и нажмите кнопку "Продолжить".

   Если при создании импортируемой конфигурации был включен параметр "Установить профиль по умолчанию" и ранее пользователем был выбран другой профиль по умолчанию, на экране появится окно с предложением изменить его.

8. Выполните одно из следующих действий:
   - для смены профиля по умолчанию нажмите кнопку "Да";
   - для продолжения работы без изменений нажмите кнопку "Нет".

   На экране появится сообщение о завершении импорта профиля.

9. Нажмите кнопку "Закрыть".

Примечание. Если профиль импортирован без сертификата или пары "логин–пароль", на экране появится сообщение о необходимости заполнить соответствующие поля в настройках профиля. Укажите сертификат и ключевой контейнер либо введите логин и пароль пользователя, а затем нажмите кнопку "Сохранить".

Если профиль настроен корректно, на экране появится сообщение с предложением произвести пробное подключение с использованием импортированного профиля.

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

    В случае установления подключения на экране появится информационное сообщение.

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

Для выбора профиля по умолчанию укажите в списке профиль и нажмите кнопку "Установить профиль по умолчанию" на панели инструментов (см. стр. **13**). В строке с профилем появится соответствующий значок. Автоматическое подключение к СД будет осуществляться по данному профилю.

Для отмены данного действия выполните одно из следующих действий:

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

Для удаления профиля подключения:

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

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

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

   Профиль будет удален из списка.

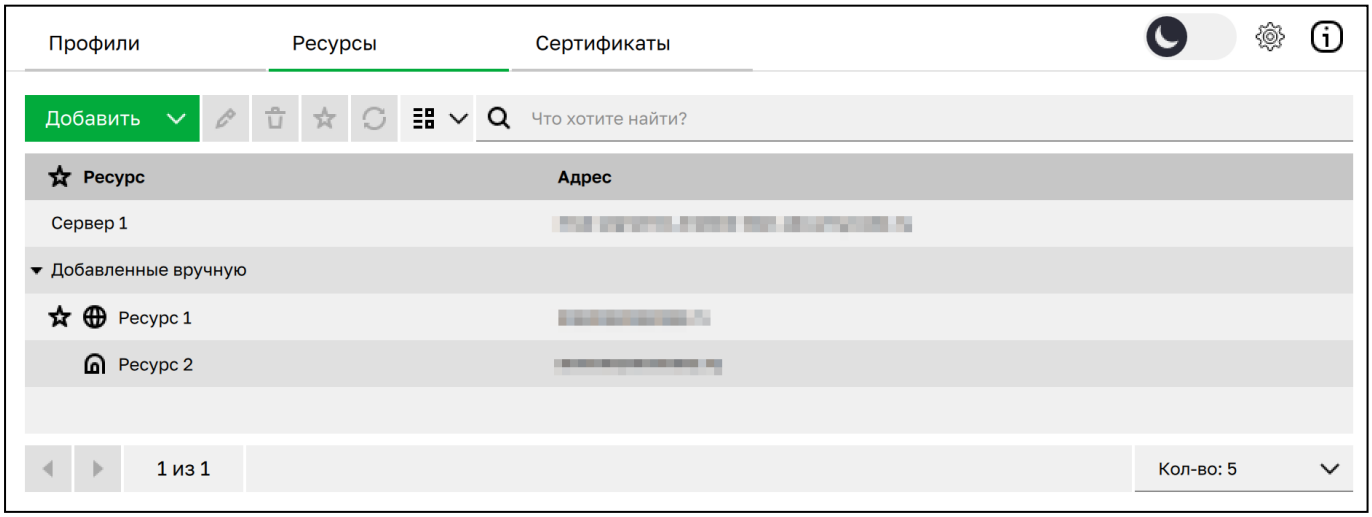
Для удаления сохраненных паролей:

1. Выберите профиль и нажмите кнопку "Удалить сохраненные пароли" на панели инструментов.
2. В появившемся раскрывающемся списке выберите один из следующих пунктов:
   - "Удалить пароль из профиля", если для выбранного профиля был сохранен пароль;
   - "Удалить все пароли" для всех профилей в списке.

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

Управление защищенными ресурсами

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



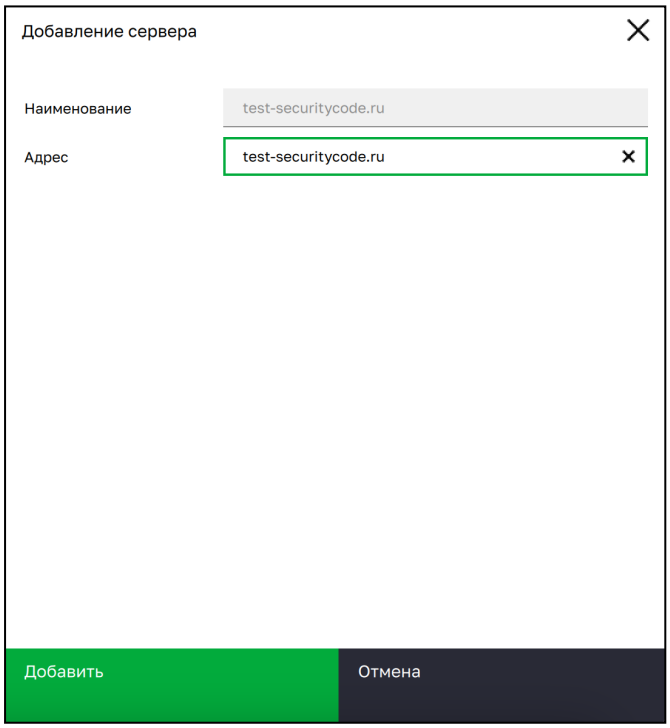
Панель инструментов раздела "Ресурсы" содержит элементы, приведенные ниже.

Кнопка	Описание
Добавить	Добавить сервер/ресурс
	Редактировать параметры сервера/ресурса
	Удалить сервер/ресурс
	Добавить ресурс в избранное
	Обновить список серверов и ресурсов
	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. **18**).
2. В появившемся раскрывающемся списке нажмите кнопку "Сервер".
   В правой части основного окна появится список настроек сервера.



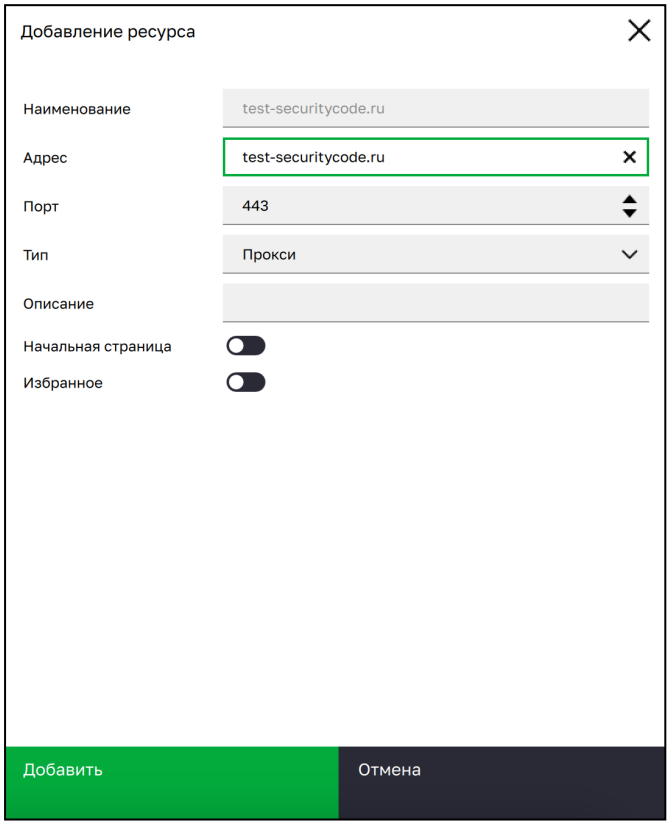
3. Введите название сервера для установления TLS-подключения в поле "Наименование".
4. Укажите сетевое имя или IP-адрес сервера в поле "Адрес".
5. Нажмите кнопку "Добавить".
   На экране появится запрос на загрузку ресурсов.
6. Нажмите кнопку "Да".
   На экране появится окно выбора сертификата для доступа к серверу.
7. Выберите из списка требуемый сертификат и нажмите кнопку "Применить".
   Ресурсы добавленного сервера будут загружены и появятся в списке.

Для добавления ресурса:

Примечание. Ресурс, загруженный ранее при добавлении сервера, добавить нельзя. В случае если сначала был добавлен ресурс, а затем — сервер с одноименным ресурсом, он будет перемещен в список ресурсов сервера.

1. В основном окне Клиента в разделе "Ресурсы" нажмите кнопку "Добавить" на панели инструментов.
2. В появившемся 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 подключения и установите значение в поле "Порт".
6. При необходимости заполните поле "Описание", а также установите отметки "Начальная страница" и "Избранное".

   Примечание. Отметки "Начальная страница" и "Избранное" доступны в случае, если в поле "Тип" указано значение "Прокси".
7. 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 изменения в доступные поля и нажмите кнопку "Сохранить".

   Изменения будут применены.

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

Для отмены данного действия выполните одно из следующих действий:

- нажмите кнопку "Добавить в избранное" повторно либо удалите отметку в настройках ресурса;
- установите отметку "Добавить в избранное" для другого ресурса с типом "Прокси" в списке.

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 окно запроса 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 общих параметров подключения (подробнее см. на стр. **33**).
2. Настройте значения параметров на требуемых вкладках и нажмите кнопку "Сохранить".

Подключение к серверу доступа

Внимание! Подключение к СД возможно только с помощью профиля, имеющего статус "Действителен".

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.
- Максимальное количество попыток ввода пароля доступа к ключевому контейнеру — 5. После 5-й неудачной попытки установление соединения с СД будет прервано.

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" и перейдите на вкладку "VPN".

   На экране появится окно настройки параметров режима VPN.
2. Установите отметку в поле "Автоматическое подключение к серверу доступа с профилем по умолчанию" (подробнее см. на стр. **33**).
3. Если при создании или импорте профилей не был назначен профиль по умолчанию, выберите один из списка и установите для него отметку "Использовать по умолчанию" (подробнее о настройке профиля см. на стр. **15**).

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

   Внимание! Если в настройках указано не разрывать соединение при выходе из программы, текущее подключение к СД останется активным в фоновом режиме (подробнее о режиме завершения работы см. на стр. **35**).

Подключение в ручном режиме

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

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

Внимание! Если ранее не был назначен профиль по умолчанию, предварительно выберите профиль из списка и установите для него отметку "Использовать по умолчанию" (подробнее о настройке профиля см. на стр. 15).

1. Запустите Континент ZTN Клиент.
2. Выполните одно из следующих действий:
   - наведите указатель на значок ПО в строке меню и дважды нажмите левой кнопкой мыши;
   - наведите указатель на значок ПО в строке меню и нажмите правую кнопку мыши. В контекстном меню выберите пункт "Подключить "<имя_профиля>".

   Начнется процесс подключения с профилем по умолчанию. При успешном подключении к СД значок в строке меню станет зеленым.

Для подключения к СД в ручном режиме из строки меню:

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в строке меню и нажмите правую кнопку мыши.
3. В контекстном меню выберите пункт "Установить соединение", а затем — имя требуемого профиля.

   Начнется процесс подключения с выбранным профилем. При успешном подключении к СД значок в строке меню станет зеленым.

Если соединение с СД установлено с помощью значка в строке меню и произошел разрыв соединения, начнется переподключение к тому же СД. При исчерпании количества попыток подключения начнется установление соединения со следующим СД из списка в профиле.

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 "Подключить" 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 в строке меню станет зеленым.

Если соединение с СД установлено из основного окна Клиента и произошел разрыв соединения, начнется переподключение к тому же СД. При исчерпании количества попыток подключения установление соединения с СД будет прервано.

Разрыв соединения с сервером доступа

Для разрыва соединения с СД из строки меню дважды нажмите левой кнопкой мыши по значку Клиента или вызовите контекстное меню и нажмите кнопку "Отключить "<имя_профиля>". Соединение с СД будет разорвано, а значок в строке меню 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 требуемый профиль и нажмите кнопку "Отключить" на панели инструментов.

   Соединение с СД будет разорвано, значок в строке меню 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.

Доступ к защищенным ресурсам

Для корректного подключения к защищенным веб-ресурсам по протоколу HTTPS необходимо импортировать в хранилище корневых сертификатов используемого веб-браузера сертификат "ContinentZTNRootCert", который расположен в файле с именем "cert" в директории "etc/cts/cert/tlsca/0000".

Примечание. Перед импортом сертификата необходимо в название файла "cert" добавить расширение "cer".

Сертификат "ContinentZTNRootCert" также необходимо импортировать в системное хранилище средствами приложения "Связка ключей".

Для импорта сертификата в системное хранилище:

Внимание! Для импорта сертификата в системное хранилище требуются права администратора.

1. В директории "etc/cts/cert/tlsca/0000" выберите файл "cert.cer", одновременно нажмите левую кнопку мыши и клавишу <control>, в контекстном меню нажмите кнопку "Открыть".
2. В появившемся окне введите пароль и нажмите кнопку "Изменить связку ключей".

   Запустится приложение "Связка ключей".
3. В списке объектов приложения "Связка ключей" дважды нажмите левой кнопкой мыши по строке с сертификатом "ContinentZTNRootCert".

   На экране появится окно со свойствами сертификата.
4. Откройте раздел "Доверие", в раскрывающемся списке "Параметры использования сертификата" укажите значение "Всегда доверять".
5. Закройте окно со свойствами сертификата.
6. В появившемся окне введите пароль и нажмите кнопку "Обновить настройки".

   Окно свойств сертификата закроется. Новые параметры сертификата будут применены.

Внимание! При повторной установке ПО Клиента необходимо заново импортировать сертификат "ContinentZTNRootCert" в системное хранилище и хранилище корневых сертификатов используемого веб-браузера.

Для доступа к избранным ресурсам из строки меню:

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

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в строке меню 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 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.

   Если не установлен сертификат по умолчанию (см. стр. 33), 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".

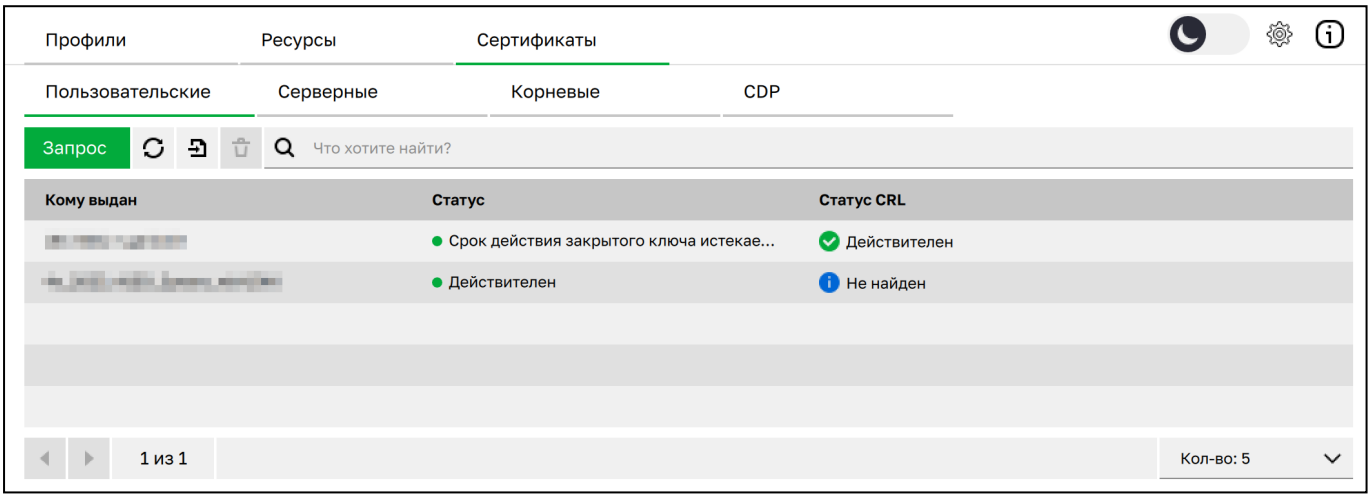
   Примечание.
   - Если требуется сохранить пароль доступа, установите отметку в соответствующем поле.
   - Если пользователь 5 раз подряд в течение 10 минут предъявил недействительный сертификат, доступ к серверу заблокируется на 10 минут (ограничение реализовано на стороне сервера, его параметры могут быть изменены).

   Окно закроется, защищенное соединение с указанным ресурсом будет установлено.

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 импортированных сертификатов/список CDP
	Импортировать сертификат/CRL
	Удалить сертификат/CDP, добавленный вручную
Добавить +	Добавить CDP вручную
	Редактировать параметры CDP, добавленного 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. **24**.

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.

После получения всех сертификатов необходимо установить их в локальное хранилище компьютера средствами Клиента (см. стр. **27**).

Для отображения состояния сертификатов используются статусы, приведенные ниже.

Активен
Сертификат действителен и используется в профиле для подключения
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
Ошибка проверки цепочки сертификатов
Не удалось построить цепочку от пользовательского сертификата до корневого
Нет CRL
Сертификат не прошел проверку по CRL, так как не импортирован необходимый CRL-файл
CRL просрочен
Срок действия CRL истек или еще не наступил
Отозван по CRL
Сертификат не прошел проверку по CRL

Создание запроса

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

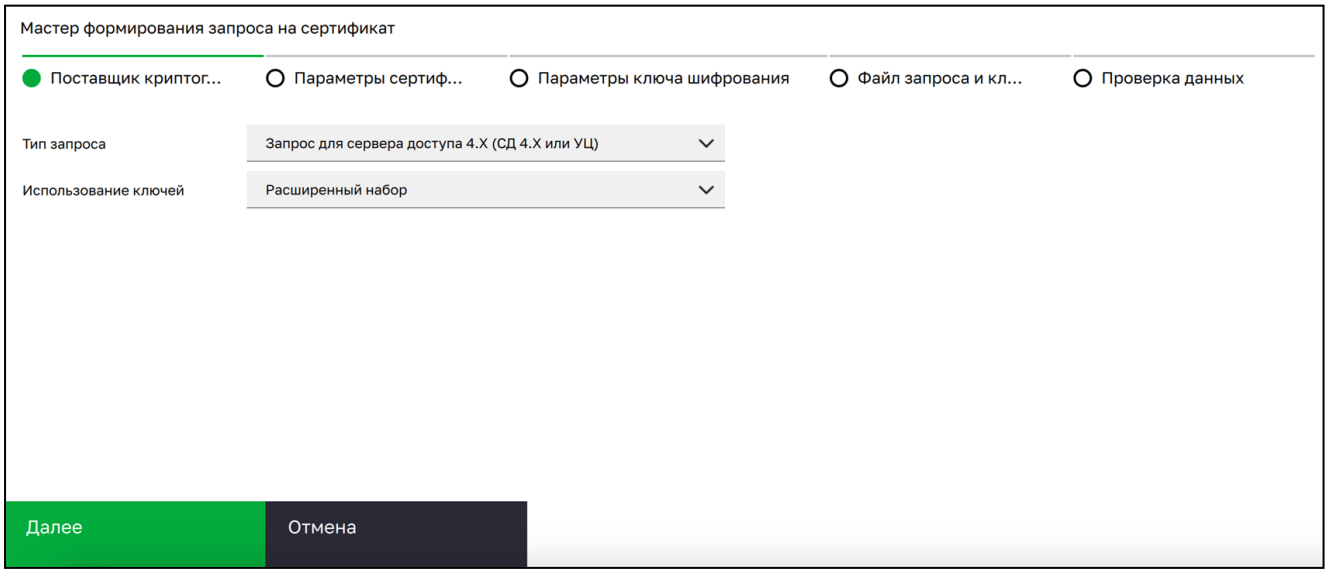
Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе, указанном в настройках.

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. **23**).

   На экране появится окно создания запроса на сертификат.



2. Выберите в раскрывающемся списке тип запроса на сертификат.

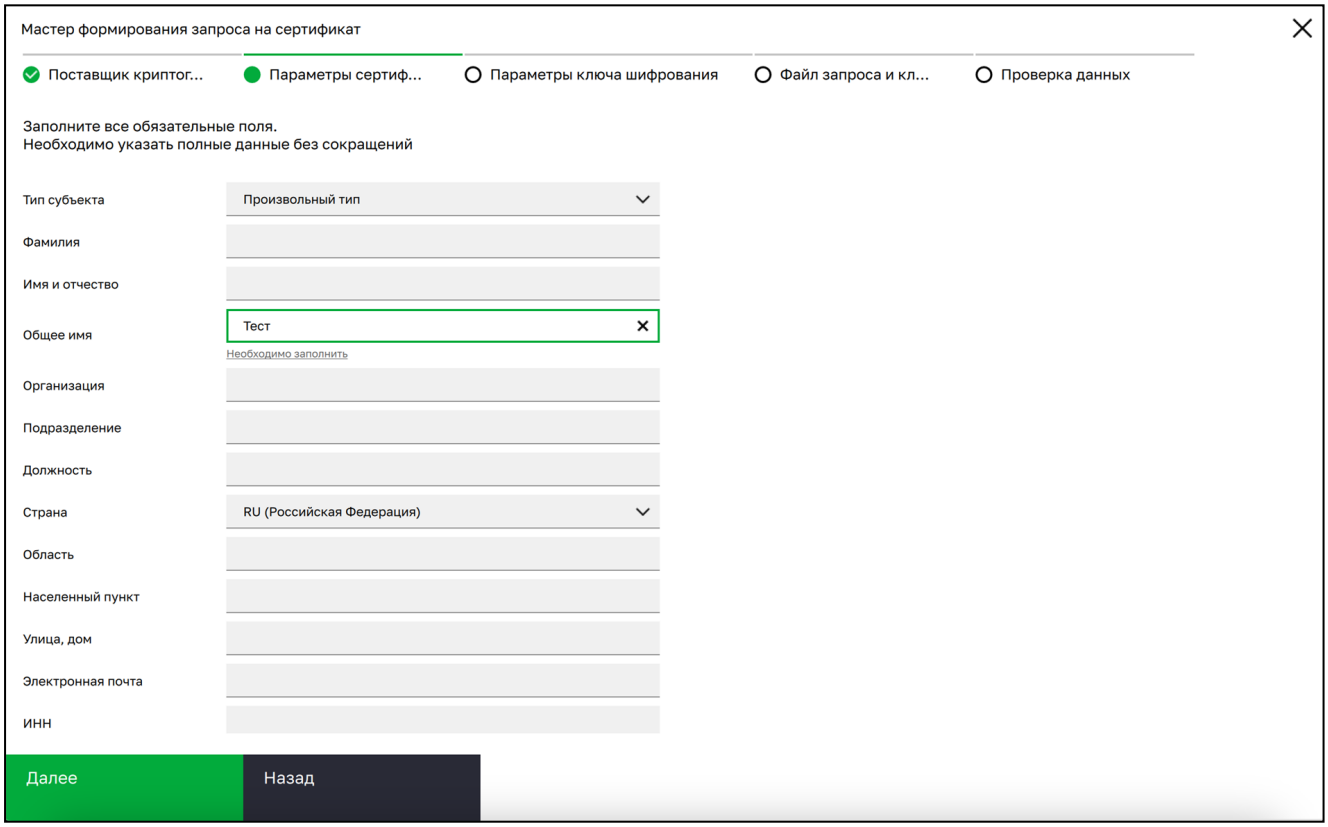
Запрос для сервера доступа 3.X (СД 3.X)
Формат запроса для выпуска сертификата в МК (или СД версии 3.9.1 в режиме работы протокола версий 4.X) или внешним центром сертификации (алгоритм по ГОСТ Р 34.10-2012)
Запрос для сервера доступа 4.X (СД 4.X или УЦ)
Формат запроса для выпуска сертификата в ПУ СД (алгоритм по ГОСТ Р 34.10-2012)

3. 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

4. Нажмите кнопку "Далее".

   На экране появится диалог для ввода параметров запроса.



5. В раскрывающемся списке "Тип субъекта" укажите требуемое значение.

   Примечание. В зависимости от значения параметра "Тип субъекта" меняются параметры формы запроса.

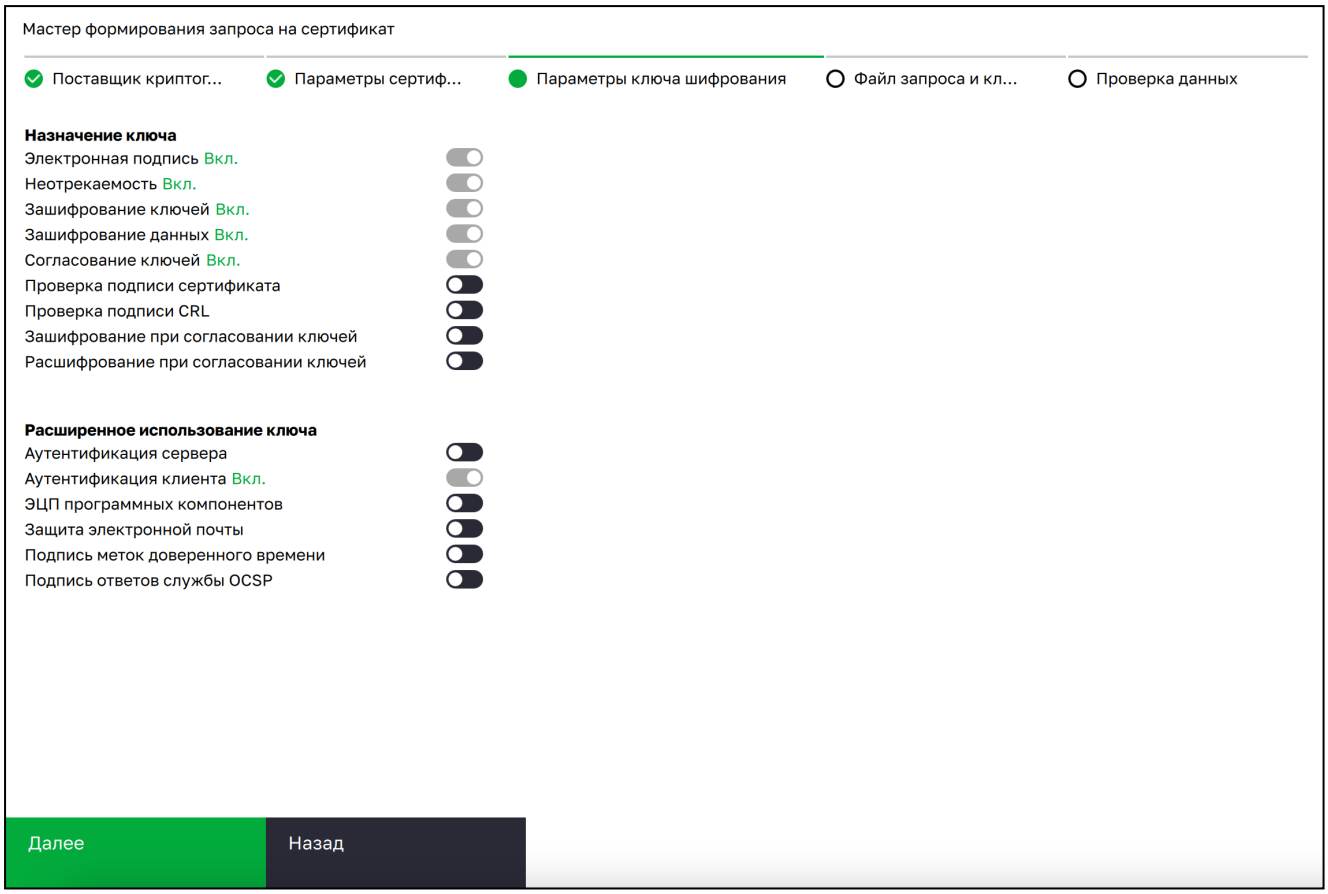
6. Укажите сведения о субъекте в оставшихся полях.

   Внимание! Для продолжения настройки запроса требуется указать значения для параметров с отметкой "Необходимо заполнить".

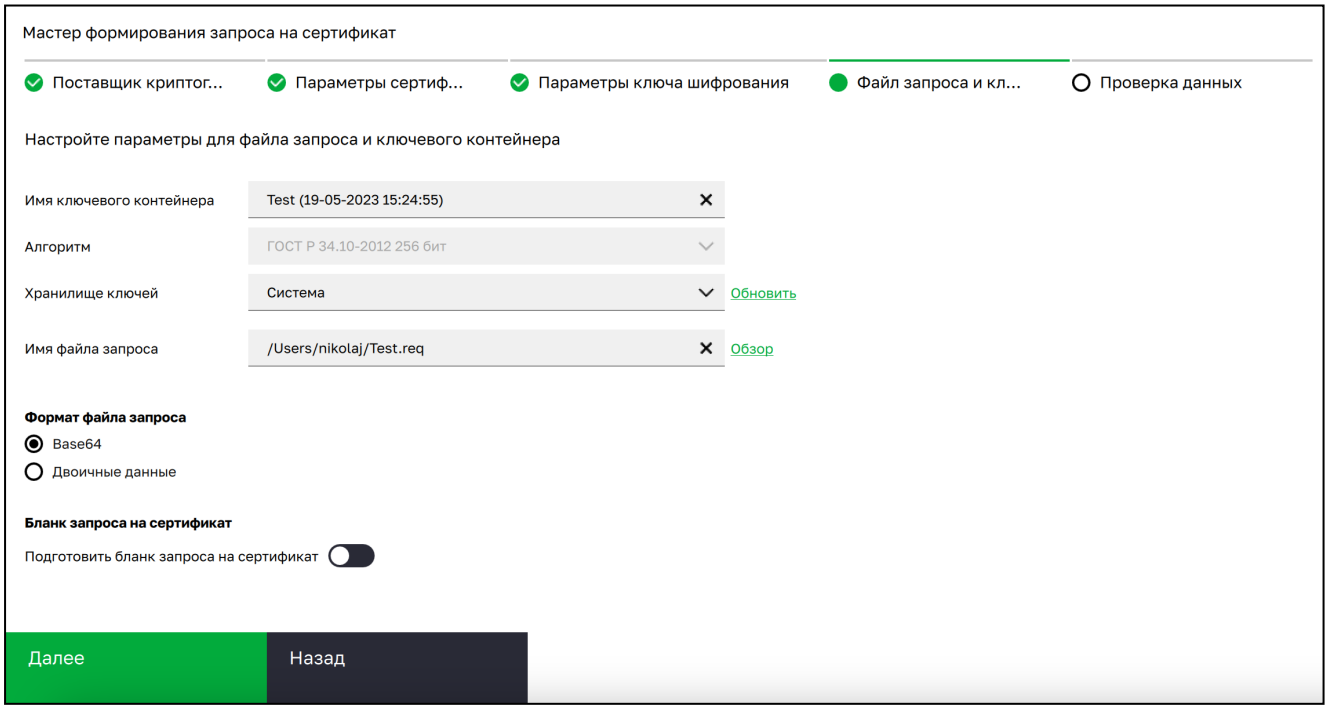
7. Нажмите кнопку "Далее".

   Если указан стандартный набор параметров использования ключа, на экране появится окно для ввода имени ключевого контейнера и имени файла для запроса сертификата. Перейдите к п. **9**.

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



8. Установите отметки для необходимых параметров ключа шифрования и нажмите кнопку "Далее".
На экране появится окно настройки свойств файла запроса и ключевого носителя.



9. 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.
- Для изменения расположения или имени файла запроса нажмите кнопку "Обзор". В открывшемся окне укажите диск (папку) для создания файла и имя файла запроса, а затем нажмите кнопку "Сохранить".

10. Выберите из раскрывающегося списка требуемый алгоритм.
11. Выберите из раскрывающегося списка "Хранилище ключей" тип ключевого носителя.

Примечание. Для корректного подключения рекомендуется сохранять ключевой контейнер в системе.

12. Выберите формат, в котором будет сохранен файл запроса.
13. Установите отметку в поле "Подготовить бланк запроса на сертификат", если необходимо сохранить версию запроса для печати.

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

14. Нажмите кнопку "Далее".

    На экране появится сообщение о завершении работы мастера запроса сертификата и отобразятся параметры создаваемого запроса.
15. Нажмите кнопку "Создать".

    Начнется процедура создания закрытого ключа. На экране появится окно накопления энтропии для биологического датчика случайных чисел.
16. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

    После завершения процедуры на экране появится окно ввода пароля доступа к ключевому контейнеру.
17. Введите и подтвердите пароль доступа к создаваемому ключевому контейнеру и нажмите кнопку "ОК".

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

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

Внимание! Если используемый съемный носитель содержит файлы, имена которых совпадают с именами записываемых файлов, файлы на этом носителе будут автоматически переименованы и сохранены.

18. Нажмите кнопку "Закрыть" и извлеките носитель, если закрытый ключ был сохранен на нем.

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

Импорт и удаление сертификатов

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

Для импорта сертификата пользователя:

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

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 стандартное окно открытия файла.
3. Выберите файл сертификата и нажмите кнопку "Открыть".

   На экране появится окно импорта сертификата.

Примечание. Для выбора другого файла сертификата нажмите кнопку "Обзор", в появившемся окне выберите требуемый файл и нажмите кнопку "Открыть".

4. Нажмите кнопку "Далее".
5. Выберите в раскрывающемся списке требуемый тип хранилища.

6. В зависимости от типа хранилища выполните одно из следующих действий:
   - файловая система — нажмите кнопку "Обзор", в появившемся окне выберите требуемый файл ключа и нажмите кнопку "Открыть";

     Внимание! При установленном значении "Файловая система" необходимо указать ключ в формате для ОС Windows.

   - хранилище — выберите хранилище ключей в раскрывающемся списке и укажите требуемый файл в области "Контейнер";

     Примечание.
     - Для обновления списка доступных хранилищ нажмите кнопку "Обновить".
     - При выборе ключевого контейнера на съемном носителе на экране появится сообщение о том, что ключ будет скопирован в системное хранилище. Для продолжения импорта нажмите кнопку "Да". В случае отказа импорт сертификатов будет прерван.

7. Нажмите кнопку "Импортировать".

   На экране появится окно ввода пароля доступа к ключевому контейнеру.

8. Введите пароль и нажмите кнопку "Продолжить".

   Начнутся загрузка и установка сертификата. Если в папке, где хранится сертификат пользователя, будет обнаружен соответствующий корневой сертификат, откроется окно с предложением его импортировать.

9. Нажмите кнопку "Да".

   На экране появится сообщение об успешном выполнении операции.

10. Нажмите кнопку "Закрыть".

Для импорта серверного/корневого сертификата:

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку с требуемым видом сертификата и нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится стандартное окно открытия файла.

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

   Сертификат появится в списке.

Для удаления сертификата пользователя:

Внимание! Сертификат пользователя не может быть удален, если он привязан к профилю подключения или установлен в качестве сертификата по умолчанию для установления TLS-соединений (см. табл. на стр. 34).

1. Если сертификат привязан к профилю подключения, выполните следующие действия:
   - в основном окне Клиента в разделе "Профили" выберите профиль, к которому привязан сертификат, и нажмите кнопку "Редактирование профиля" на панели инструментов.

     На экране появится список настроек профиля.

   - выберите другой возможный сертификат пользователя и нажмите кнопку "Сохранить".
2. Если сертификат установлен в качестве сертификата по умолчанию для установления TLS-соединений, выполните следующие действия:
   - в основном окне Клиента в разделе "Настройки" перейдите на вкладку "TLS";
   - выберите другой возможный сертификат пользователя в поле "Сертификат по умолчанию".
3. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "Пользовательские сертификаты".

   В области отображения информации появится список установленных сертификатов.

4. Выберите сертификат и нажмите кнопку "Удалить" на панели инструментов.
5. В окне подтверждения нажмите кнопку "Удалить".

   Сертификат будет удален из списка.

Для удаления корневого/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 требуемый сертификат и нажмите кнопку "Удалить".
3. В окне подтверждения нажмите кнопку "Удалить".

   Сертификат будет удален из списка.

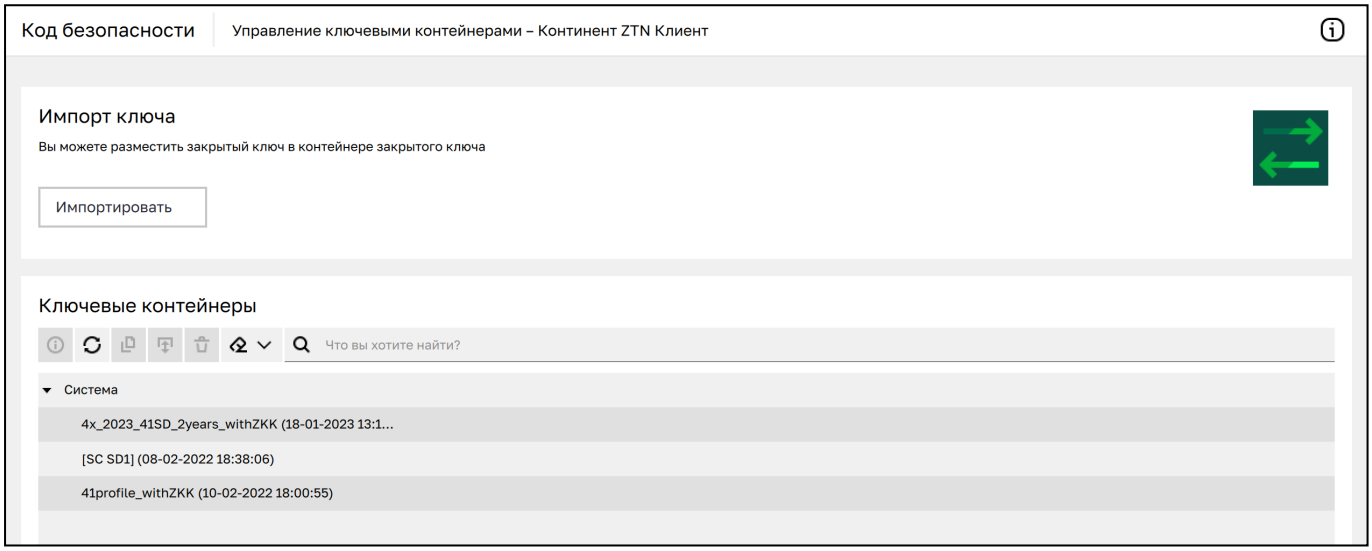
Импорт закрытого ключа

Континент ZTN Клиент может использовать закрытые ключи, созданные на других компьютерах с помощью других ОС.

Администратор безопасности формирует ключевой контейнер с закрытым ключом пользователя, сохраняет его на отчуждаемом носителе и вместе с паролем передает пользователю или администратору Клиента. Для работы с таким ключом необходимо предварительно выполнить операцию импорта закрытого ключа.

Операция импорта заключается в преобразовании формата ключа и сохранении его в локальном хранилище компьютера или на внешнем носителе.

Управление ключами осуществляется с помощью утилиты "Управление ключевыми контейнерами – Континент ZTN Клиент". Окно утилиты содержит область для импорта ключа и область просмотра импортированных ключевых контейнеров, включающую в себя панель инструментов и строку поиска.



Панель инструментов области "Ключевые контейнеры" содержит элементы, приведенные ниже.

Кнопка	Описание
	Просмотр информации о ключевом контейнере
	Обновление списка ключевых контейнеров
	Копирование ключевого контейнера
	Перемещение ключевого контейнера
	Удаление ключевого контейнера
	Удаление сохраненных паролей ключевого контейнера либо всех паролей

Для импорта закрытого ключа:

1. Вставьте ключевой носитель, полученный от администратора безопасности.
2. Откройте меню "Launchpad" и выберите приложение "Управление ключами".
   На экране появится окно утилиты импорта ключей.
3. Нажмите кнопку "Импортировать".
   На экране появится окно параметров импорта закрытого ключа.
4. В поле "Закрытый ключ" нажмите кнопку "+".
   На экране появится окно выбора закрытого ключа.

5. В раскрывающемся списке выберите хранилище ключей, укажите ключ и нажмите кнопку "Выбрать".
6. В поле "Ключевое хранилище" нажмите кнопку "+".
   На экране появится окно выбора хранилища для хранения ключевого контейнера.
7. Выберите хранилище, в которое будет сохранен ключевой контейнер, и нажмите кнопку "Выбрать".
8. Нажмите кнопку "Импортировать".
9. Следуйте указаниям инструкции на экране и дождитесь завершения операции.
   Импортируемый ключ будет сохранен.

Для просмотра списка ключевых контейнеров нажмите кнопку "▶" в строке "Система".

Для просмотра сведений о ключевом контейнере выберите в списке контейнер и нажмите кнопку "Информация" на панели инструментов (см. выше) либо нажмите дважды левой кнопкой мыши по требуемой строке. На экране появится окно со сведениями о ключевом контейнере.

Для обновления списка ключевых контейнеров нажмите кнопку "Обновить" на панели инструментов.

Для копирования ключевого контейнера:

1. В окне утилиты импорта ключей выберите в списке требуемый ключевой контейнер.
2. Нажмите кнопку "Копировать" на панели инструментов.
   На экране появится окно копирования ключевого контейнера.
3. Нажмите кнопку "+" для выбора ключевого хранилища.
   На экране появится окно выбора хранилища.

   Примечание. Для обновления списка доступных хранилищ нажмите соответствующую кнопку.
4. Укажите требуемое хранилище и нажмите кнопку "Выбрать".
5. Нажмите кнопку "Копировать".
   На экране появится сообщение об успешном выполнении операции.
6. Нажмите кнопку "Закрыть".

Для перемещения ключевого контейнера:

1. В окне утилиты импорта ключей выберите в списке требуемый ключевой контейнер.
2. Нажмите кнопку "Переместить" на панели инструментов.
   На экране появится окно перемещения ключевого контейнера.
3. Нажмите кнопку "+" для выбора ключевого хранилища.
   На экране появится окно выбора хранилища.

   Примечание. Для обновления списка доступных хранилищ нажмите соответствующую кнопку.
4. Укажите требуемое хранилище и нажмите кнопку "Выбрать".
5. Нажмите кнопку "Переместить".
   На экране появится сообщение об успешном выполнении операции.
6. Нажмите кнопку "Закрыть".

Для удаления ключевого контейнера:

1. В окне утилиты импорта ключей выберите в списке требуемый ключевой контейнер.
2. Нажмите кнопку "Удалить ключ" на панели инструментов.
   На экране появится окно запроса на подтверждение операции.
3. Нажмите кнопку "Удалить".

Для удаления сохраненных паролей:

1. В окне утилиты импорта ключей выберите требуемый ключевой контейнер.
2. Нажмите кнопку "Удалить сохраненные пароли" на панели инструментов.
3. В появившемся раскрывающемся списке выберите один из следующих пунктов:
   - "Удалить сохраненные пароли ключа", если для выбранного контейнера был сохранен пароль;
   - "Удалить все сохраненные пароли" для всех ключей в списке.

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

Просмотр сведений о сертификатах

Получить информацию об импортированных сертификатах можно с помощью средств Клиента.

Для просмотра сведений о сертификате:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку с требуемым типом 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 информации о сертификате нажмите кнопку "Закрыть".

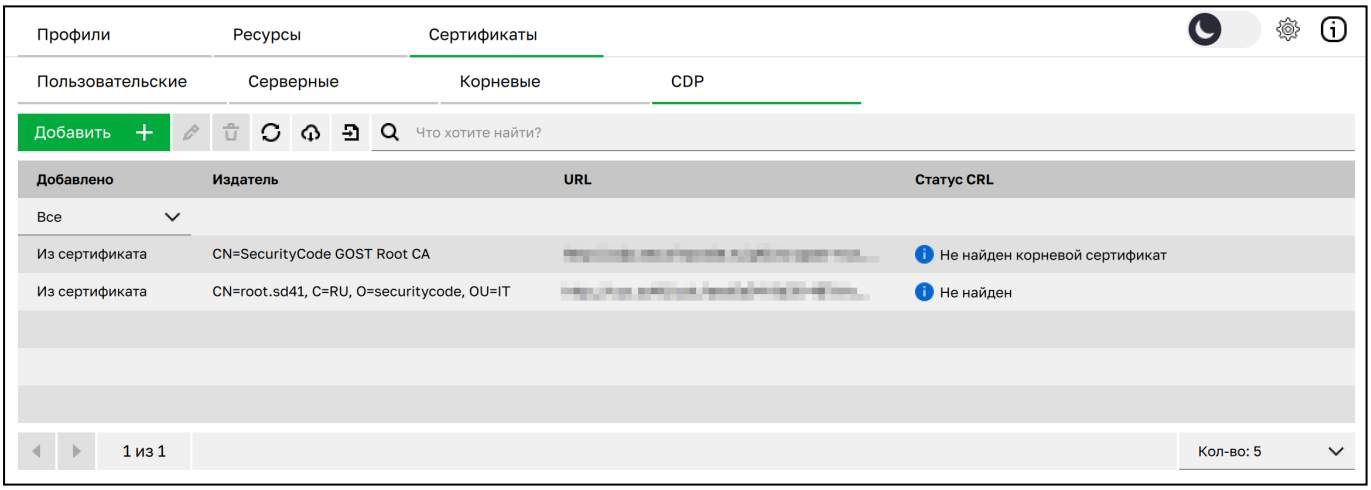
Управление CRL

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. **23**).

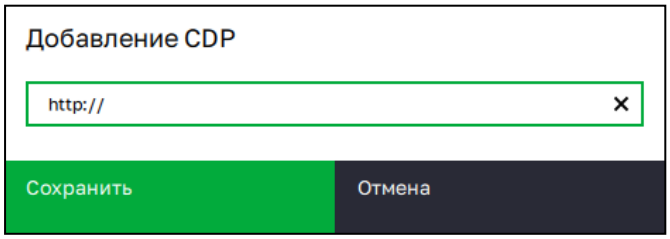
Настройка CDP

Если используемые сертификаты содержат информацию о CDP, Континент ZTN Клиент получит ее при импорте сертификатов. Для автоматической загрузки CRL из CDP необходимо импортировать пользовательский, корневой или серверный сертификат (см. стр. **27**) или добавить CDP вручную (см. ниже).



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. **23**).
   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 выберите раздел "Сертификаты" и перейдите на вкладку "CDP".
   В области отображения информации появится список используемых CDP.
2. Нажмите кнопку "Редактировать" на панели инструментов.
   На экране появится окно редактирования CDP.
3. Внесите требуемые изменения и нажмите кнопку "Сохранить".
   Изменения будут применены.

Для удаления CDP:

Примечание. Удаление CDP, полученного из сертификата, невозможно.

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".
   В области отображения информации появится список используемых CDP.
2. Выберите требуемый CDP и нажмите кнопку "Удалить" на панели инструментов.
   На экране появится запрос на подтверждение операции.
3. Нажмите кнопку "Удалить".
   CDP будет удален из списка.

Для обновления списка CDP необходимо использовать кнопку "Обновить" на панели инструментов.

Загрузка CRL

Автоматическая загрузка CRL происходит в результате добавления CDP вручную и/или после импорта сертификатов. CRL также может быть добавлен вручную с помощью кнопки "Загрузить".

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 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".
   На экране появится стандартное окно открытия файла.
3. Укажите требуемый CRL-файл и нажмите кнопку "Открыть".
   Начнется загрузка. После завершения операции на экране появится соответствующее сообщение.

   Примечание. Если для CRL совпадает издатель, будет загружен наиболее актуальный.
4. Нажмите кнопку "Закрыть".

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. 31).
2. Нажмите кнопку "Загрузить" на панели инструментов.
   Начнется загрузка. После завершения операции на экране появится соответствующее сообщение.
3. 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 общих параметров Клиента:

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

Параметр	Описание
Режим запуска	
При запуске системы	При включенном параметре ПО Клиента запускается автоматически после загрузки ОС
Свернуть в системный трей при запуске	При включенном параметре Клиент запускается в свернутом виде, в строке меню появляется значок Клиента
Подтверждение	
Подтверждать сброс соединений	При включенном параметре в случае разрыва соединения по инициативе пользователя на экране появится окно подтверждения

3. Нажмите кнопку "Сохранить".

Настройки сертификатов и CRL

Внимание! Для изменения настроек сертификатов и CRL требуются права администратора. Для настройки параметров нажмите кнопку в нижней части окна, в открывшемся окне введите пароль учетной записи администратора и нажмите кнопку "Продолжить".

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, приведенных ниже.

Параметр	Описание
Пользовательские сертификаты	
Предупреждать об истечении срока действия	Начало периода оповещения пользователя об окончании срока действия сертификата. Принимает значения от 1 до 30 (в днях)
Запрашивать добавление других серверных сертификатов	При включенном параметре во время первого подключения к СД для добавления сертификата в локальное хранилище запрашивается подтверждение пользователя. При отказе пользователя установление соединения будет прервано
Закрытый ключ	
Предупреждать об истечении срока действия	Начало периода оповещения пользователя об окончании срока действия закрытого ключа. Принимает значения от 1 до 30 (в днях)
Параметры CRL	
Проверять подлинность сертификатов	При включенном параметре во время установления соединения с СД и/или ресурсами осуществляется проверка подлинности сертификатов по CRL

Параметр	Описание
Блокировать работу при истечении срока действия CRL	Период, в течение которого возможно осуществить подключение после истечения срока действия CRL. Принимает значения 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 (см. выше). Принимает значения от 1 до 48 (в часах). Доступно для настройки только при включенном параметре "Автоматическая загрузка CRL"

3. Нажмите кнопку "Сохранить".

Настройки TLS-соединений

Внимание! Для изменения некоторых настроек установления TLS-подключения требуются права администратора. Для настройки параметров нажмите кнопку в нижней части окна, в открывшемся окне введите пароль учетной записи администратора и нажмите кнопку "Продолжить".

Для настройки параметров работы режима TLS:

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

В области отображения информации появится окно настройки режима TLS.

2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Пользовательские сертификаты	
Сертификат по умолчанию	Сертификат, который будет автоматически использоваться для подключения к ресурсам. При нажатии кнопки "..." открывается окно ранее импортированных сертификатов, для выбора сертификата необходимо нажать кнопку "Применить"
Сбросить	Нажмите кнопку "Сбросить", если необходимо сбросить выбранный сертификат в поле "Сертификат по умолчанию"
Параметры шифронаборов	
Использовать шифронабор Магма	Управление использованием шифронаборов "Магма" и "Кузнечик"
Использовать шифронабор Кузнечик	
Серверные сертификаты	
Проверять подлинность сертификатов	При включенном параметре во время установления соединения с СД и/или ресурсами осуществляется проверка подлинности сертификатов по CRL
Обновление списка ресурсов	
Проверить наличие обновлений	При нажатии кнопки, если доступно обновление списка ресурсов, на экране появится окно с соответствующим уведомлением. При нажатии кнопки "Да" осуществляется обновление списка ресурсов
Автоматически проверять наличие обновлений	При включенном параметре осуществляется автоматическая проверка обновления списка ресурсов с периодичностью, указанной в параметре "Периодичность проверки", и временем ожидания, указанным в параметре "Тайм-аут соединения"
Периодичность проверки	Период времени для автоматического обновления ресурсов (в часах). Принимает значения от 1 до 999. Значение по умолчанию — 1
Тайм-аут соединения	Период времени ожидания сервера при обновлении списка ресурсов (в секундах). Принимает значения от 1 до 999. Значение по умолчанию — 120

Параметр	Описание
Подключение	
Протокол	Используемая версия TLS-протокола. 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 VPN

Внимание! Для изменения некоторых настроек установления VPN-подключения требуются права администратора. Для настройки параметров нажмите кнопку в нижней части окна, в открывшемся окне введите пароль учетной записи администратора и нажмите кнопку "Продолжить".

Для настройки параметров работы режима VPN:

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 осуществляется автоматическое подключение к СД с профилем по умолчанию (подробнее о настройке профиля см. на стр. **16**)
Режим завершения	
Разорвать все соединения	При включенном параметре 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, соединения с ресурсами прервутся
Параметры шифронаборов	
Использовать шифронабор Магма	Управление использованием шифронаборов "Магма" и "Кузнечик"
Использовать шифронабор Кузнечик	

3. Нажмите кнопку "Сохранить".

Настройки прокси-сервера

Внимание! Данные настройки прокси-сервера будут использоваться при соединении с СД и 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-сервера	При включенном параметре используются системные настройки прокси и становится недоступен параметр "Подключаться через внешний прокси-сервер", а также остальные поля для настройки прокси-сервера
Подключаться через внешний прокси-сервер	При включенном параметре в полях ниже становится доступна ручная настройка прокси-сервера для установления соединения с СД и ресурсами. Недоступно при включенном параметре "Автоматически определять настройки прокси-сервера"

Параметр	Описание
Адрес	Адрес прокси-сервера (URL или IP-адрес)
Порт	Порт прокси-сервера. Принимает значения от 1 до 65535
Исключения	Адреса веб-ресурсов, для подключения к которым не используется внешний прокси-сервер
Аутентификация	
Метод аутентификации	Метод аутентификации на прокси-сервере. Принимает значения: • автоматически; • без аутентификации; • Basic; • NTLM; • Negotiate
Использовать данные текущего пользователя системы	При включенном параметре аутентификация на прокси-сервере осуществляется с помощью учетных данных текущего пользователя ОС, указываемых в полях ниже
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 осуществляется сброс пароля к внешнему прокси-серверу

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:

Примечание. Конфигурация содержит данные о профилях и ресурсах пользователя, от имени которого осуществлен вход в систему.

1. В окне настроек перейдите на вкладку "Конфигурация".
2. В группе параметров "Экспорт" в раскрывающемся списке выберите требуемый тип данных:
   - полная конфигурация;
   - профили подключения и настройки;
   - список ресурсов и настройки;
   - сертификаты.
3. Нажмите кнопку "Экспортировать".

   В зависимости от типа данных на экране может появиться сообщение о том, что пользовательские сертификаты или ключевые контейнеры экспортированы не будут.
4. При необходимости нажмите кнопку "Да".

   На экране появится стандартное окно для сохранения файла.
5. Укажите имя файла и его месторасположение, а затем нажмите кнопку "Сохранить".

   На экране появятся сообщение об успешном выполнении операции и предложение открыть папку расположения файла конфигурации для сохранения файлов ключей.
6. Нажмите кнопку "Да" для сохранения файлов ключей в папке с файлом конфигурации.

Для импорта конфигурации:

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

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

   При импорте полной конфигурации или файлов сертификатов на экране появится сообщение о необходимости использования носителя с закрытыми ключами.

При импорте файла, содержащего настройки и профили/списки ресурсов, перейдите к п. **5**.

4. Нажмите кнопку "Да".

   На экране появится сообщение о необходимости ввода пароля администратора для импорта некоторых настроек.

   Примечание. При нажатии кнопки "Нет" выполнение операции продолжится, но импорт параметров, для изменения которых требуются права администратор, осуществлен не будет.

5. Нажмите кнопку "Да".

   На экране появится окно ввода пароля учетной записи администратора.

6. Введите пароль администратора и нажмите кнопку "Продолжить".

   При импорте полной конфигурации или файлов сертификатов на экране появится окно импорта сертификата.

   При импорте файла, содержащего настройки и профили/списки ресурсов, перейдите к п. **10**.

7. Укажите требуемые значения в полях "Хранилище" и "Ключевой контейнер".

   Примечание. Для обновления списка доступных хранилищ нажмите кнопку "Обновить".

8. Нажмите кнопку "Импортировать".

   На экране появится окно ввода пароля доступа к ключевому контейнеру.

9. Введите пароль к ключевому контейнеру и нажмите кнопку "ОК".

   Конфигурация будет импортирована. На экране появится соответствующее сообщение.

10. Нажмите кнопку "Закрыть".

Просмотр событий

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

При экспорте диагностической информации выполняется сохранение архива, содержащего следующие файлы:

- журнал событий, связанных с работой Клиента в режиме VPN — cts.log;
- журнал событий, связанных с работой Клиента в режиме TLS — ctstls.log;
- файлы настроек Клиента;
- файлы сертификатов (цепочка пользовательских сертификатов без ключевого контейнера, цепочка серверных сертификатов);
- файлы дампов памяти (если при экспорте была установлена отметка, см. ниже).

Для просмотра событий необходимо открыть требуемый файл журнала в текстовом редакторе.

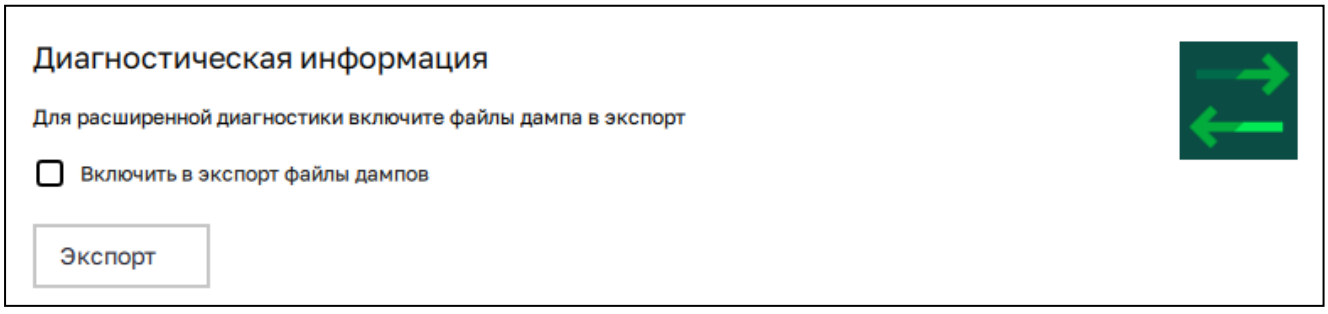
Для каждого события приводятся следующие сведения:

- дата и время;
- код и категория события;
- имя пользователя (для событий, инициированных пользователем);
- краткое описание события.

Для сбора диагностической информации:

1. Откройте меню "Launchpad" и выберите приложение "Диагностика".

   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 "Экспорт".

   На экране появится стандартное окно сохранения файла.

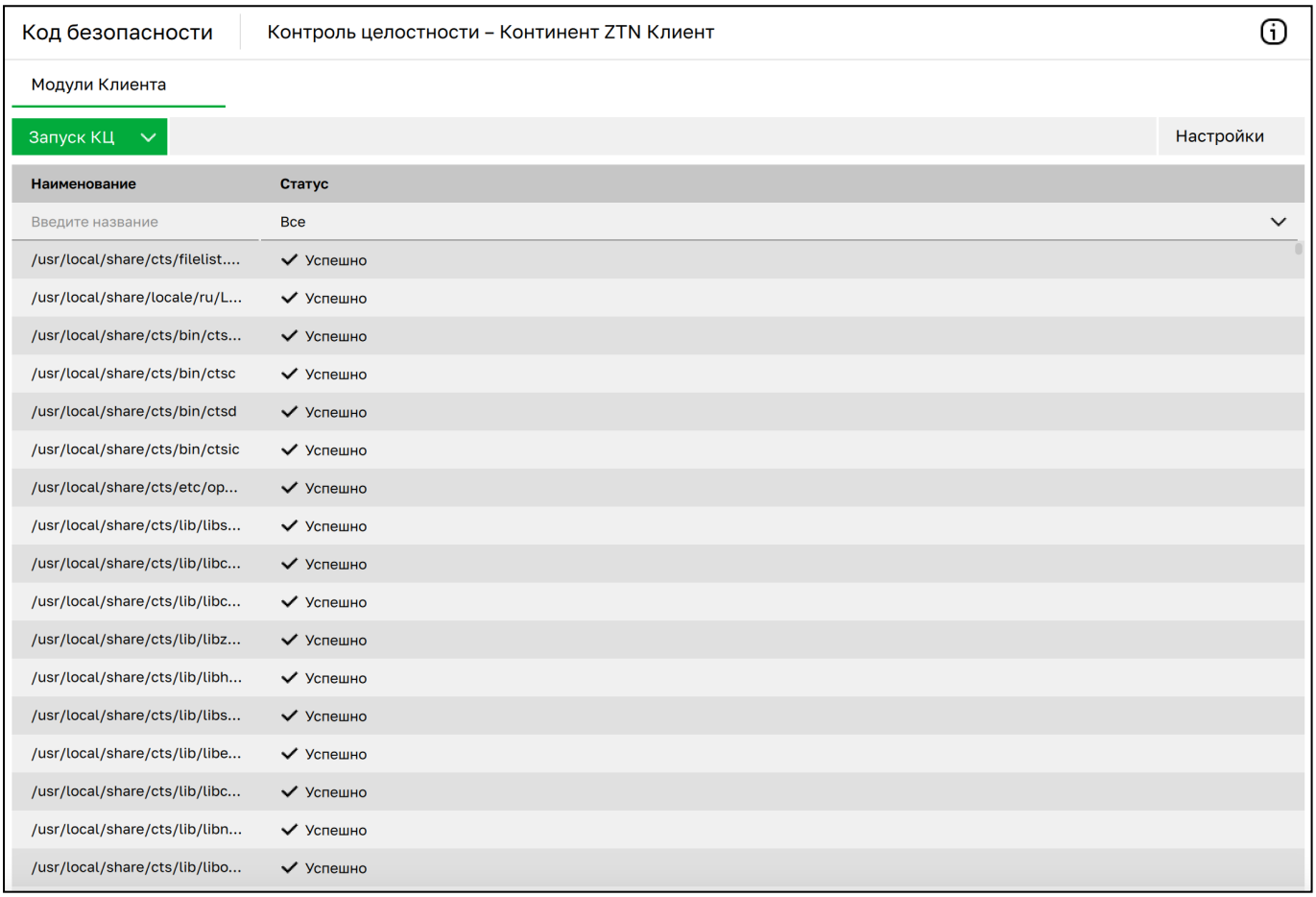
4. Укажите имя архива и его месторасположение, а затем нажмите кнопку "Сохранить".

   На экране появится сообщение об успешном выполнении операции.

5. Нажмите кнопку "Закрыть".

Контроль целостности

Контроль целостности осуществляется с помощью утилиты "Контроль целостности – Континент ZTN Клиент". При запуске утилиты проверка КЦ начнется автоматически, статусы контролируемых файлов в списке будут обновлены.



Для проверки целостности вручную:

1. Откройте меню "Launchpad" и выберите приложение "Контроль целостности".

   На экране появится основное окно УКЦ.

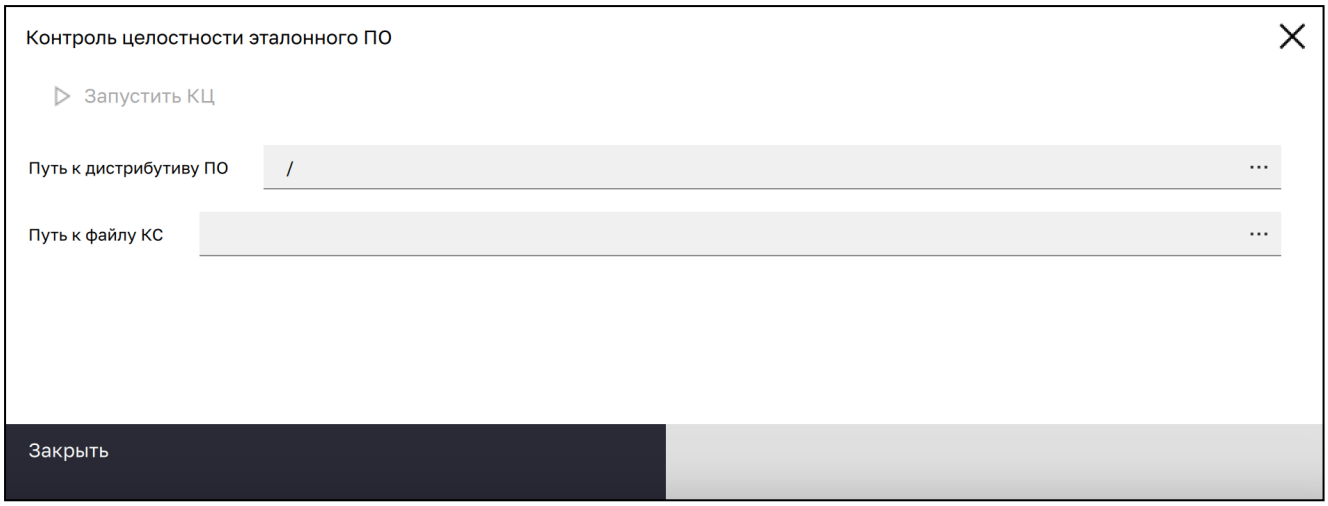
2. На панели инструментов нажмите кнопку "Запуск КЦ".
3. В раскрывающемся списке нажмите кнопку "Программа".

   Начнется процедура проверки целостности, по завершении которой будут обновлены статусы контролируемых файлов.

Для проверки целостности эталонного ПО:

1. В основном окне УКЦ 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. Укажите пути к дистрибутиву ПО и файлу КС в соответствующих полях, нажав кнопку "...".
4. Нажмите кнопку "Запустить КЦ".

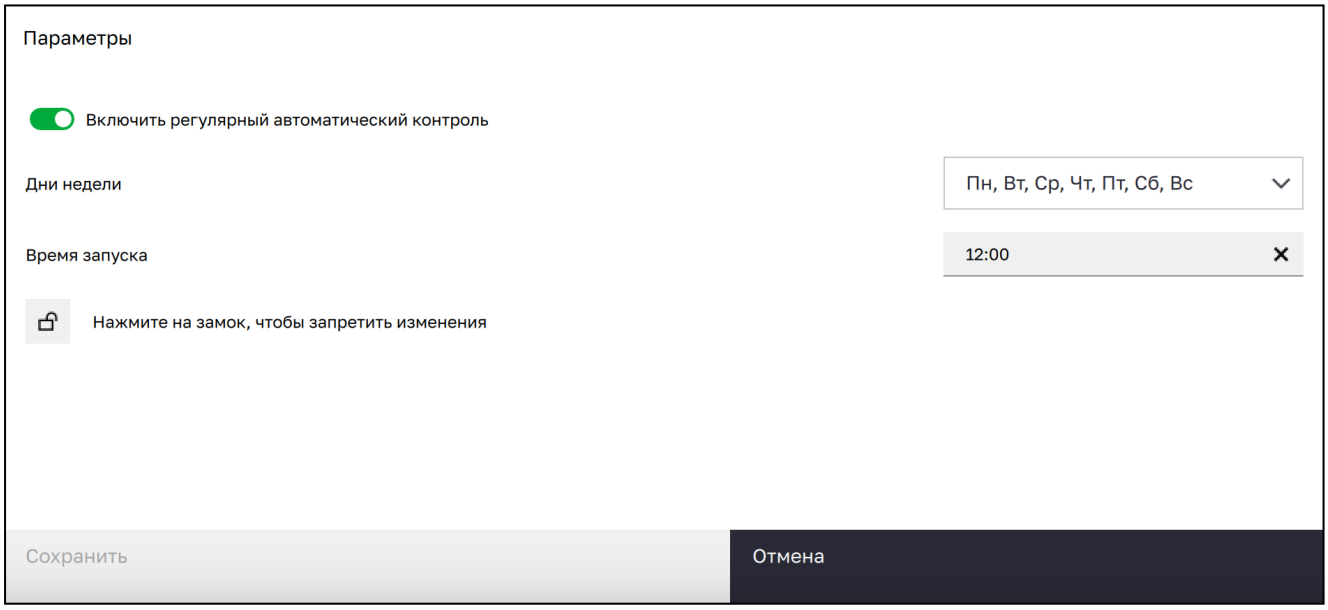
   Начнется процедура проверки целостности эталонного ПО, в результате которой на экране появится таблица, содержащая названия проверенных файлов, их контрольные суммы и статусы КЦ.

Для настройки проверки целостности по расписанию:

Примечание. Для настройки проверки целостности по расписанию требуются права администратора.

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

   На экране появится окно с настройками расписания автоматической проверки целостности.



2. Нажмите кнопку для внесения изменений в настройки.

   На экране появится окно ввода пароля учетной записи администратора.
3. Введите пароль администратора и нажмите кнопку "Продолжить".
4. Активируйте параметр "Включить регулярный автоматический контроль".

   Параметры "Дни недели" и "Время запуска" станут доступными для настройки.
5. В раскрывающемся списке "Дни недели" укажите требуемые значения.
6. В поле "Время запуска" укажите время для начала процедуры проверки целостности по расписанию.
7. Нажмите кнопку "Сохранить".

   Автоматическая проверка целостности будет осуществляться по указанному расписанию.

Окно "О программе"

Окно "О программе" содержит сведения о текущей версии ПО "Континент ZTN Клиент" и позволяет пользователю связаться со службой технической поддержки.

Для обращения в службу технической поддержки:

Примечание. Для обращения в службу технической поддержки необходимо предварительно выполнить экспорт архива с диагностической информацией (см. стр. 37).

1. В основном окне Клиента в правом верхнем углу нажмите кнопку ⓘ.
   На экране появится окно со сведениями о текущей версии Клиента.
2. Нажмите на адрес технической поддержки в области "Обратная связь".
   На экране появится окно выбора способа отправки файла.
3. Выберите требуемый почтовый клиент.
   В появившемся окне автоматически будут заполнены строки "От", "Кому" и "Тема".
4. Прикрепите экспортированный ранее архив с диагностической информацией и отправьте письмо.

Приложение

Управление Клиентом из командной строки

В данном разделе приведено описание специализированной утилиты **cts**, используемой для управления Клиентом. Для управления Клиентом из командной строки выполните одно из следующих действий:

- откройте меню "Launchpad" и выберите приложение "Терминал";
- в окне "Finder" перейдите по пути "Программы" | "Утилиты" и выберите приложение "Терминал".

Утилита вызывается в следующем формате:

```
cts команда [-параметр 1] [-параметр 2]... [-параметр n]
```

Для каждой команды имеется уникальный набор параметров. Список команд и их описание приведены в таблице ниже.

Команда	Описание
help/--help/-help/-h	Вызов инструкции по использованию утилиты
version/--version/-version/-v	Просмотр версии Клиента
connect	Подключение к СД
disconnect	Отключение от СД
request	Создание запроса на сертификат
import key	Импорт закрытого ключа
import profile	Импорт профиля из файла конфигурации
events	Просмотр журнала событий
show profile	Просмотр параметров профиля
show certificate/cert	Просмотр данных сертификата
show config/parameter	Просмотр конфигурации пользователя
show stats	Просмотр статистики подключений
show settings	Просмотр всех текущих настроек
show settings general	Просмотр текущих основных настроек
show settings proxy	Просмотр текущих настроек прокси
show settings gui	Просмотр текущих настроек графического интерфейса приложения
show cdp	Просмотр списка CDP
add profile	Создание профиля пользователя
add connection	Добавление подключения к СД в существующий профиль пользователя
add cert	Добавление сертификата
add cdp	Добавление адреса CDP
edit/modify profile	Редактирование профиля пользователя
edit/modify connection	Редактирование параметров подключения к СД для профиля
edit/modify cdp	Редактирование адреса CDP
edit/modify config/parameter	Редактирование конфигурации пользователя
edit/modify settings proxy	Редактирование настроек прокси
edit/modify settings general	Редактирование основных настроек
edit/modify settings gui	Редактирование настроек графического интерфейса приложения

Команда	Описание
delete/del profile	Удаление профиля пользователя
delete/del connection	Удаление подключения к СД для профиля
delete/del cdp	Удаление адреса CDP
delete/del cert	Удаление сертификата
delete/del pass	Удаление пароля (паролей)
update crl	Обновление списка отозванных сертификатов

Команда connect

Команда осуществляет подключение к СД. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-profile <NAME>	Имя профиля подключения
-password/-pass	Пароль профиля
-pin	PIN-код контейнера
-store-password	Сохранить пароль после успешного подключения
-store-pin	Сохранять PIN-код после успешного подключения

Команда disconnect

Команда осуществляет отключение от СД. Принимает на вход опциональный параметр -profile <NAME> для указания имени профиля.

Команда request

Команда предназначена для создания запроса на сертификат. В ходе выполнения команды будет выполнен диалоговый скрипт для получения данных о пользователе, набора энтропии и выбора ключевого носителя для сохранения на нем закрытого ключа.

Команда import key

Команда осуществляет импорт закрытого ключа. В ходе выполнения команды будет выполнен диалоговый скрипт для выбора ключевого носителя с закрытым ключом, хранилища для импортируемого ключа и набора энтропии. Принимает на вход обязательный параметр -ras-version/-ras <number {3, 4}> для указания версии СД.

Команда import profile

Команда осуществляет импорт конфигурационного файла профиля. В ходе выполнения команды будет выполнен диалоговый скрипт. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательный	
-file-path/-path	Путь к файлу
Опциональные	
-file-pass	Пароль доступа к файлу
-key-pass	Пароль ключевого контейнера
-ras-version/-ras {3, 4}	Версия СД

Команда events

Команда предназначена для просмотра журнала событий. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-category/-cat {INFO, ERROR, DEBUG}	Категория события
-start-time/-from <dd.mm.yyyy:hh:mm:ss>	Время начала
-end-time/-to <dd.mm.yyyy:hh:mm:ss>	Время окончания
-user <NAME>	Имя пользователя

Команда show profile

Команда предназначена для просмотра списка профилей. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-name <regular_expression>	Имя профиля
-server <regular_expression>	IP-адрес сервера
-user <NAME>	Имя пользователя

Команда show certificate/cert

Команда предназначена для просмотра информации о сертификатах. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-type {user, ca, as, crl}	Тип сертификата
-subject-cn <regular_expression>	Имя владельца сертификата
-subject-org <regular_expression>	Организация владельца сертификата
-issuer-cn <regular_expression>	Имя издателя сертификата
-issuer-org <regular_expression>	Организация издателя сертификата
-user <NAME>	Имя пользователя
-hide-expired	Скрывать просроченные сертификаты

Команда show config/parameter

Команда предназначена для просмотра информации о конфигурации пользователя. Принимает на вход опциональный параметр -user <NAME> для указания имени пользователя.

Команда show stats

Команда предназначена для просмотра информации об активном подключении. Принимает на вход опциональный параметр -user <NAME> для указания имени пользователя.

Команда add profile

Команда предназначена для создания профиля подключения. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля

Параметр	Описание
Опциональные	
-ras-version/-ras {3, 4}	Версия СД
-auth {login, cert}	Тип аутентификации
-cert-path	Путь к сертификату
-login	Логин пользователя
-server <HOST>	Адрес сервера (только для СД версий 3.X)
-port <number {0..65535}>	Порт сервера доступа (только для СД версий 3.X)
-proto/-protocol	Протокол соединения
-user <NAME>	Имя пользователя
-default	Использовать профиль по умолчанию
-select-cert	Выбрать сертификат
-select-key	Выбрать ключевой контейнер

Внимание!

- Один из параметров — логин пользователя или путь до сертификата — является обязательным.
- Если при подключении имя пользователя должно вводиться в формате domain\user, необходимо использовать следующий синтаксис: domain\\user.

Команда add connection

Команда предназначена для добавления подключения в существующий профиль. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательные	
-profile <NAME>	Имя профиля
-server <HOST>	Адрес сервера
Опциональные	
-name <NAME>	Имя соединения
-user <NAME>	Имя пользователя
-port <number {0..65535}>	Порт СД
-number <number {1..}>	Порядковый номер соединения

Команда add cert

Команда предназначена для добавления сертификатов. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательные	
-type {user, ca, as, crl}	Тип сертификата
-path	Путь к сертификату
Опциональный	
-user	Имя пользователя

Команда add cdp

Команда предназначена для ручного добавления адреса CDP. Принимает на вход обязательный параметр -url <URL> для указания адреса CDP.

Команда edit/modify profile

Команда предназначена для редактирования профиля пользователя. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля
Опциональные	
-ras-version/-ras {3, 4}	Версия СД
-auth {login, cert}	Тип аутентификации
-cert-path	Путь к сертификату
-login	Логин пользователя
-server <HOST>	Адрес сервера (только для СД версий 3.X)
-port <number {0..65535}>	Порт сервера доступа (только для СД версий 3.X)
-proto/-protocol	Протокол соединения
-user <NAME>	Имя пользователя
-default	Использовать профиль по умолчанию
-select-cert	Выбрать сертификат
-select-key	Выбрать ключевой контейнер

Команда edit/modify connection

Команда предназначена для редактирования существующего подключения в профиле. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательные	
-profile <NAME>	Имя профиля
-name <NAME>	Имя соединения
Опциональные	
-user <NAME>	Имя пользователя
-server <HOST>	Адрес сервера
-port <number {0..65535}>	Порт СД
-number <number {1..}>	Порядковый номер соединения

Команда edit/modify cdp

Команда предназначена для редактирования адреса CDP, введенного вручную. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательные	
-number/-N <number {1..}>...	Номер CDP
-url	Ссылка на CDP

Команда edit/modify config/parameter

Команда предназначена для редактирования конфигурации пользователя. Принимает на вход опциональный параметр -connection-try-count <number {0..99}> для указания количества попыток подключения.

Команда edit/modify settings proxy

Команда предназначена для настройки прокси соединения. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-use <boolean {on, off, yes, no}>	Использовать/не использовать прокси
-server <HOST>	Адрес прокси-сервера
-port <number {0..65535}>	Порт прокси-сервера
-auth {no (default), basic, ntlm}	Тип аутентификации прокси-сервера
-domain	Домен пользователя
-login	Логин пользователя
-password	Пароль пользователя

Команда edit/modify settings general

Команда предназначена для изменения основных настроек приложения. Принимает на вход опциональный параметр -cert-warning-days <дн. {1..30}> для изменения количества дней до появления уведомления об истечении срока действия сертификата.

Команда edit/modify settings gui

Команда предназначена для изменения графических настроек приложения. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-auto-connect <boolean {true, false, no, yes, y, n, on, off}>	Автоматическое подключение с профилем по умолчанию при запуске графического приложения
-auto-disconnect <boolean {true, false, no, yes, y, n, on, off}>	Автоматически разрывать соединение при выключении графического приложения
-color-theme {light, dark}	Тема оформления графического приложения
-minimize-on-start <boolean {true, false, no, yes, y, n, on, off}>	При запуске графического приложения свернуть в системный трей

Команда delete/del profile

Команда предназначена для удаления профиля пользователя. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля
Опциональный	
-user <NAME>	Имя пользователя

Команда delete/del connection

Команда предназначена для удаления существующего подключения в профиле. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательные	
-profile <NAME>	Имя профиля

Параметр	Описание
-name <NAME>	Имя соединения
Опциональный	
-user <NAME>	Имя пользователя

Команда delete/del cdp

Команда предназначена для удаления адреса CDP, введенного вручную. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-number, -N <number {1..}>	Номер CDP
-url	Ссылка на CDP

Команда delete/del cert

Команда предназначена для удаления сертификатов. Принимает на вход параметры, указанные ниже (требуется использовать как минимум один опциональный параметр).

Параметр	Описание
Обязательный	
-type {user, ca, as, crl}	Тип сертификата
Опциональные	
-user	Имя пользователя
-subject-cn <regular_expression>	Имя владельца сертификата
-subject-org <regular_expression>	Организация владельца сертификата
-issuer-cn <regular_expression>	Имя издателя сертификата
-issuer-org <regular_expression>	Организация издателя сертификата

Команда delete/del pass

Команда предназначена для удаления сохраненных паролей из профилей пользователя. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Опциональные	
-profile <NAME>	Имя профиля
-all	Удаление паролей из всех профилей пользователя