

Континент ZTN Клиент для Windows

Комментарии к сборке 4.4.0.77

Документ содержит описание основных возможностей, особенностей работы и ограничений применения изделия "Континент ZTN Клиент для Windows" (далее — Континент ZTN Клиент, Клиент, изделие), которые необходимо учитывать при его эксплуатации.

Список сокращений

ДСЧ	Датчик случайных чисел
ЗПС	Замкнутая программная среда
ОС	Операционная система
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
CRL	Certificate Revocation List (список отозванных сертификатов)
DNS	Domain Name System (система доменных имен)

Оглавление

1.	Изменения и новые возможности	3
1.1.	Версия 4.4.0.77.....	3
1.2.	Версия 4.3.15.43.....	3
2.	Требования к аппаратному и программному обеспечению	4
3.	Особенности работы и ограничения.....	5

1. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях Клиента версии 4.4.0.77.

1.1. Версия 4.4.0.77

1. Удалена поддержка ГОСТ Р 34.11-94.
2. Удалена поддержка ГОСТ Р 34.10-2001.
3. Реализован механизм настройки использования протокола TLS 1.0.
4. Реализован механизм настройки использования алгоритмов ГОСТ 28147-89.
5. Реализована поддержка совместной работы с СКЗИ "КриптоПро CSP".
6. Реализован механизм уведомления администратора об истечении сроков действия сертификатов и закрытых ключей. Уведомление осуществляется за указанный администратором период времени (в днях) до окончания сроков действия сертификатов и закрытых ключей.
7. При совместной работе с СЗИ Secret Net Studio реализована возможность создания ЗПС.
8. Реализован механизм ролевой аутентификации – поддерживается работа в ролях пользователя и администратора (привилегированный пользователь).
9. Реализован механизм пересчета КС модулей ОС, в среде которой функционирует Клиент. Процедура перерасчета КС доступна всем пользователям в исполнениях, соответствующих классам КС1 и КС2; в исполнениях, соответствующих классу КС3 – только администратору.

1.2. Версия 4.3.15.43

1. Реализована возможность управления Клиентом с помощью пользовательского графического интерфейса с настраиваемыми цветовыми схемами (светлая и темная) и командной строки.
2. Реализована возможность установления защищенного соединения с СД 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").
3. Реализована возможность установления защищенного соединения с изделием "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее – СКЗИ "Континент TLS-сервер") и обмена данным с веб-серверами корпоративной сети.
4. Реализован механизм регистрации событий, связанных с работой Клиента.
5. Реализована возможность сбора и экспорта на внешний носитель журналов событий, файлов расширенного логирования, дампов памяти, конфигурации и сертификатов.
6. Реализован механизм контроля целостности файлов ПО Клиента и связанных с ним файлов ОС.
7. Реализован механизм регистрации ПО Клиента.
8. Реализована возможность запрета незащищенных соединений при подключении к СД.

2. Требования к аппаратному и программному обеспечению

1	Ключевые устройства	• 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; • USB-флеш-накопитель
2	Операционная система	• Windows 10 x86/x64 (не ниже версии 1909); • Windows 11 x64; • Windows Server 2016 x64; • Windows Server 2019 x64
3	Совместимое программное обеспечение	• ПАК "Соболь"; • СЗИ Secret Net Studio; • СКЗИ "КриптоПро CSP" 4.0, 5.0; • СКЗИ "Валидата CSP" 6; • Kaspersky Endpoint Security; • Kaspersky Internet Security; • Dr.Web Security Space; • Avast Internet Security; • ESET NOD32 Internet Security

3. Особенности работы и ограничения

1. Управление соединениями с TLS-ресурсами осуществляется только с помощью пользовательского графического интерфейса.
2. Подключение до входа в систему не поддерживается при использовании ключевых устройств "Рутокен" с ключевыми контейнерами, сформированными средствами СКЗИ "КриптоПро CSP" (далее — КриптоПро CSP).
3. При совместной работе с КриптоПро CSP для осуществления соединений с СД до входа в систему требуется предварительно установить отметку запоминания пароля доступа к ключевому контейнеру, который используется для подключения.
4. Клиентом не поддерживается совместная работа ключевых устройств "JaCarta" и "Esmart" с ключевыми контейнерами, сформированными средствами КриптоПро CSP.
5. Клиентом не поддерживается работа с сертификатами, в которых используются разные алгоритмы ключей издателя и конечного сертификата.
6. Для работы с сертификатами ГОСТ Р 34.10-2012 (512 бит) требуется КриптоПро CSP или расширенная лицензия eXtended Container.
7. Не рекомендуется использовать Клиент в среде ОС Windows с неоригинальными (сторонними) языковыми стандартами. В противном случае в работе Клиента могут возникать ошибки.
8. Совместная работа Клиента и КриптоПро CSP версии 4 не поддерживается на компьютерах, функционирующих под управлением ОС Windows 11. Для совместной работы КриптоПро CSP и Клиента в среде ОС Windows 11 необходимо использовать КриптоПро CSP версии 5.0. В противном случае могут возникнуть ошибки "Не удалось установить TCP-соединение с сервером <имя_сервера>" и/или "Затребованный пакет безопасности не существует" при совместной работе с СКЗИ "КриптоПро CSP".
9. Для изменения класса защиты (KC1/KC2/KC3) и типа ДСЧ, используемого на установленном Клиенте, необходимо удалить Континент ZTN Клиент и Код Безопасности CSP, а затем осуществить их повторную установку, выбрав необходимый класс защиты.
10. Совместная работа Континент ZTN Клиент и Рутокен S не поддерживается на компьютерах, функционирующих под управлением ОС Windows 11.
11. При использовании ключевых носителей с двумя интерфейсами (например, JaCarta-2 PKI/ГОСТ) Континент ZTN Клиент поддерживает работу только с одним из интерфейсов.
12. Если DNS-сервер недоступен во время запуска Клиента, после восстановления работоспособности DNS-сервера необходимо завершить работу Клиента и осуществить его повторный запуск.
13. При создании запроса на сертификат значение параметра "Общее имя" не должно содержать более 227 символов. В противном случае работа Клиента может завершиться ошибкой.
14. При наборе энтропии рекомендуется осуществлять нажатия в разные области мишеней. В противном случае возможны ошибки при выпуске сертификатов на сторонних УЦ и осуществлении соединений с использованием сертификата, выпущенного средствами ПУ СД.
15. В случае возникновения повышенной нагрузки на производительность процессора при открытом основном окне Континент ZTN Клиент рекомендуется свернуть/закрыть основное окно Клиента. Работа Клиента продолжится, доступ к настройкам осуществляется с помощью значка в области уведомлений панели задач ОС Windows.
16. При совместной работе с КриптоПро CSP параметры использования шифронаборов не применяются при осуществлении подключений.
17. Для корректного отображения состояния целостности файлов при открытой УКЦ необходимо завершить работу утилиты, а затем — повторно ее запустить.
18. При одновременном использовании двух DNS-серверов в списке TLS-ресурсов могут отображаться индикаторы ошибок. Подключения к таким ресурсам осуществляются корректно. Для корректного отображения TLS-ресурсов в списке рекомендуется указывать их в системном файле "hosts".
19. При первом импорте конфигурации на Клиенте с расширенной поддержкой ключевых контейнеров рекомендуется не осуществлять пробное подключение с использованием импортированного профиля. В противном случае может появиться ошибка "Не сохранен пароль ключевого контейнера". Для осуществления подключения к СД нажмите кнопку "Подключиться" на панели инструментов раздела "Профили".
20. Экспорт данных в сетевые каталоги не поддерживается утилитой "Сбор диагностической информации — Континент ZTN Клиент".

- 21.** В случае отсутствия съемного носителя с ключевым контейнером в момент установления соединения с TLS-ресурсом сообщение об ошибке не отображается, а доступ к ресурсу не осуществляется. Для доступа к ресурсу необходимо предъявить съемный носитель с ключевым контейнером.
- 22.** При создании запроса на сертификат для субъекта типа "Юридическое лицо" в случае возврата в окно "Параметры сертификата пользователя" необходимо убедиться, что в поле "ИНН ЮЛ" указаны корректные данные.

Компания "Код Безопасности"

Почтовый адрес:	115127, Россия, Москва, а/я 66
Телефон:	8 495 982-30-20
E-mail:	info@securitycode.ru
Сайт:	https://www.securitycode.ru