

Континент ZTN Клиент для Linux

Комментарии к сборке 4.4.1.194

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

Список сокращений

ОС	Операционная система
ПО	Программное обеспечение
СД	Сервер доступа
CRL	Certificate Revocation List (список отозванных сертификатов)

Оглавление

1.	Изменения и новые возможности	3
1.1.	Версия 4.4.1.194.....	3
1.2.	Версия 4.3.0.201.....	3
2.	Ограничения на поддержку аппаратных и программных средств	4
3.	Особенности работы и ограничения.....	5

1. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях Клиента версии 4.4.1.194.

1.1. Версия 4.4.1.194

1. Реализован механизм контроля качества связи.
2. Реализована поддержка функционирования Клиента на устройстве MIG T10 PRO.
3. Реализована поддержка ГОСТ Р 34.12-2015.

1.2. Версия 4.3.0.201

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 данными 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. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства	• JaCarta PKI; • JaCarta PKI/Flash; • JaCarta PKI/BIO; • JaCarta ГОСТ; • JaCarta PKI/ГОСТ; • JaCarta PKI/BIO/ГОСТ; • JaCarta ГОСТ/Flash; • Рутокен ЭЦП 2.0; • JaCarta-2 PKI/ГОСТ; • JaCarta-2 PKI/BIO/ГОСТ; • JaCarta SF/ГОСТ; • JaCarta PRO; • JaCarta-2 PRO/ГОСТ; • JaCarta LT; • Рутокен ЭЦП PKI; • Рутокен ЭЦП 2.0 Flash; • Рутокен ЭЦП 2.0; • Рутокен ЭЦП 3.0 NFC; • Рутокен Lite; • Рутокен 2151; • ESMART Token; • ESMART Token ГОСТ
2	Операционная система	• Astra Linux Common Edition 2.12.43 x86_64 Desktop; • Astra Linux Common Edition 2.12.45.5 Desktop; • Astra Linux Special Edition 1.6 x86_64 Desktop; • Astra Linux Special Edition 1.7 x86_64 Desktop; • Astra Linux Special Edition 8.1 x86_64 Desktop; • CentOS 7.2 x86_64 Server, Desktop; • CentOS 7.3.1611 x86_64 Server, Desktop; • CentOS 7.5.1804 x86_64 Server, Desktop; • Debian 11 x86_64 Server, Desktop; • RHEL 8.2 x86_64 Server, Desktop; • Ubuntu 22.04.3 LTS x86_64 Server, Desktop; • Альт Линукс 8 СП x86_64 Server, Desktop; • Альт Рабочая станция 9.1 x86_64 Desktop; • Альт Рабочая станция 9.2 x86_64 Desktop; • Альт Рабочая станция К 9.2 x86_64 Desktop; • РЕД ОС 7.3 x86_64 Server, Desktop

3. Особенности работы и ограничения

1. Для корректной работы изделия необходимо выполнить перезагрузку компьютера после установки ПО Клиента.
2. Максимальный срок действия закрытого ключа пользователя – 15 месяцев от даты его формирования. По истечении этого срока работа с сертификатом будет невозможна. Необходимо осуществить перевыпуск сертификата пользователя с закрытым ключом.
3. При работе с MIG T10 PRO, функционирующим под управлением ОС Astra Linux 1.7 в мобильном режиме, перед началом эксплуатации Континент ZTN Клиент необходимо осуществить одно из следующих действий:
 - на другом устройстве средствами Клиента осуществите набор энтропии в графическом режиме (мишени), перенесите файл формата "p15" и файл формата "p15info" (если необходимо использовать ключ формата "p15" для подключений), расположенные в "/home/<user>/.ztn", на планшетный компьютер и импортируйте перенесенный файл формата "p15" на экране импорта начальной энтропии.
 - в командной строке ОС выполните команду "cts generate-entropy".
4. При работе с MIG T10 PRO, функционирующим под управлением ОС Astra Linux 1.7 в мобильном режиме, для настройки параметров ПО Клиента, доступных только администратору:
 - 1) В главном окне Клиента перейдите в "Настройки | Общие", в области "Режим запуска" выберите параметры "При старте системы" и "Свернуть в системный трей при запуске" и нажмите кнопку "Сохранить".
 - 2) Перезагрузите устройство и запустите Континент ZTN Клиент в режиме администратора.
5. Для завершения работы ПО Клиента на MIG T10 PRO, функционирующем под управлением ОС Astra Linux 1.7 в мобильном режиме, в командной строке ОС выполните команду "killall ctsg".
6. Не рекомендуется использовать маршрут "0.0.0.0" для перенаправления всего трафика в туннель.
7. Не рекомендуется осуществлять импорт профилей подключения на устройствах с процессором Baikal, используя xrdp. Возможны ошибки в отображении ключевых носителей.
8. Импорт конфигурации из json-файла не позволяет импортировать сертификаты, т. е. при таком импорте корневые, серверные и пользовательские сертификаты добавлены не будут.
9. В случае возникновения проблем при сборе диагностической информации рекомендуется осуществлять процедуру с root-правами.
10. Установление повторного соединения с защищенными ресурсами на устройствах с процессором Baikal может завершиться ошибкой. Для установления повторного соединения необходимо осуществить перезапуск службы "ctstls", выполнив команду "sudo systemctl restart ctstls.service".
11. Если в настройках Клиента активирована автоматическая загрузка CRL, возможна задержка в работе ПО Клиента при установлении первого соединения с помощью значка на панели задач после входа в систему.
12. Работа с Клиентом в режиме администратора недоступна пользователям с низким уровнем целостности.
13. Для создания ключей на ESMART Token 64K необходимо инициализировать ключевой носитель в профилях ViPNet или ViPNet SM.
14. Средствами утилиты управления Клиентом из командной строки невозможно установить соединение с СД с использованием профиля, название которого содержит пробелы.

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