Континент ZTN Клиент для macOS
Комментарии к сборке 4.0.0.5857

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

Список сокращений

ЗНС	Запрет незащищенных соединений
ЗР	Защищенный ресурс
ОС	Операционная система
ПО	Программное обеспечение
СД	Сервер доступа
CDP	CRL Distribution Point (точка распространения списков отозванных сертификатов)
CRL	Certificate Revocation List (список отозванных сертификатов)

Оглавление

1. Изменения и новые возможности 3
1.1. Версия 4.0.0.5857 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 4.0.0.5857.

1.1. Версия 4.0.0.5857

1. 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").
2. Реализован механизм управления списком профилей подключения к СД.
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 управления списком ЗР для соединений в режиме TLS.
5. Реализован механизм управления списком сертификатов.
6. Реализована возможность создания запросов на выпуск сертификатов.
7. Реализована возможность управления Клиентом с помощью пользовательского графического интерфейса с настраиваемыми цветовыми схемами (светлая и темная) и командной строки.
8. Реализован механизм регистрации событий, связанных с работой Клиента.
9. Реализована возможность сбора и экспорта на внешний носитель журналов событий, файлов расширенного логирования, дампов памяти, конфигурации и сертификатов.
10. Реализован механизм контроля целостности файлов ПО Клиента.
11. Реализована возможность запрета незащищенных соединений при подключении к СД.
12. Реализован механизм управления списком CDP.
13. Реализован механизм автоматического обновления CRL.
14. Реализована возможность выбора протокола, используемого для соединений в режиме TLS.
15. Реализована возможность настройки автоматического подключения с профилем по умолчанию.
16. Реализована возможность управления настройками прокси-сервера.

2. Ограничения на поддержку аппаратных и программных средств

1	Ключевой носитель	USB-флеш-накопитель
2	Операционная система	• macOS Catalina (10.15); • macOS Big Sur (11); • macOS Monterey (12); • macOS Ventura (13)

3. Особенности работы и ограничения

1. Не поддерживается создание запроса на выпуск сертификата ГОСТ 34.10-2012 (512 бит).
2. С 1 января 2020 года на территории РФ запрещено формирование электронной подписи с помощью ключей электронной подписи ГОСТ Р 34.10-2001. Работа с такими сертификатами не поддерживается. Необходимо использовать ключи электронной подписи ГОСТ Р 34.10-2012.
3. Соединения, при которых осуществляется туннелирование всего трафика, не поддерживаются.
4. В работе механизма автоматического обновления списка ЗР режима TLS возможны ошибки. Рекомендуется осуществлять обновление списка ЗР вручную.
5. Невозможно установить соединение с использованием сертификата, ключевой контейнер которого распложен на съемном носителе.
6. При использовании ЗНС могут возникать ошибки доступа к ресурсам TLS-сервера. При совместном использовании режимов VPN и TLS рекомендуется не использовать ЗНС на СД.
7. В работе механизма автоматической загрузки CRL по расписанию и из CDP, полученных в результате импорта корневых и серверных сертификатов, возможны ошибки. Рекомендуется осуществлять обновление (загрузку) CRL вручную.
8. При подключении к TLS-ресурсам по протоколу https в браузере может возникать ошибка "Подключение не защищено".
9. Распространение дистрибутива Клиента рекомендуется осуществлять средствами официального веб-сайта компании "Код Безопасности" и/или USB-флеш-накопителя. В противном случае ввиду особенностей macOS при установке Клиента может возникнуть ошибка о том, что новая версия Клиента уже установлена в системе.

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