Континент ZTN Клиент для iOS, iPadOS
Комментарии к релизу 4.4.0.5821

Данный документ содержит описание возможностей изделия "Континент ZTN Клиент для iOS, iPadOS" (далее — Континент ZTN Клиент, Клиент, приложение) релиза 4.4.0.5821, а также особенностей и ограничений, которые необходимо учитывать при его эксплуатации.

Оглавление

1. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях Клиента версии 4.4.0.5821.

1.1. Версия 4.4.0.5821

1. Реализована возможность установления 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" Защищенное соединение осуществляется по протоколу версий 4.X.

2. Реализована возможность установления защищенного соединения с изделием "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее – TLS-сервер) и обмена данными с веб-серверами корпоративной сети.

3. Реализованы возможности для управления сертификатами:

- выбор пользовательского сертификата для установления соединений;
- информирование о состоянии импортированных сертификатов;
- просмотр сведений о сертификате;
- удаление пользовательских сертификатов;
- импорт файла CRL;
- проверка действительности сертификатов по CRL.

4. Реализованы возможности для управления списком профилей — создание, настройка и удаление профилей подключения.

5. Реализованы возможности для управления списком защищенных ресурсов — добавление, настройка и удаление TLS-серверов и ресурсов, а также обновление списка ресурсов, передаваемых TLS-серверами.

6. Для управления приложением реализованы режим работы с доступом ко всем настройкам (основной) и пользовательский режим (режим ограниченной функциональности).

7. Реализована возможность аутентификации на СД по пользовательскому сертификату, а также по логину и паролю.

8. Реализована возможность импорта конфигурации в приложении с помощью одного файла.

9. Реализована возможность регистрации событий на устройстве и отправки журнала по электронной почте.

10. Реализован механизм контроля целостности файлов ПО Клиента.

2. Ограничения на поддержку аппаратных и программных средств

Операционная система	• iOS 14–16; • iPadOS 14–16

3. Особенности работы и ограничения

1. При активном подключении в режиме TLS обновление списка защищенных ресурсов, передаваемых TLS-сервером, осуществляется путем разрыва текущего соединения и повторного подключения, в результате которого список обновится.

2. После перезагрузки устройства при установленном соединении с СД в Центре уведомлений устройства может отображаться сообщение о последнем успешном соединении. Актуальные сведения о состоянии подключений приводятся на главном экране приложения.

3. При подключении к веб-ресурсу в режиме VPN с включенным параметром "Соединение по запросу" рекомендуется в настройках профиля, используемого для таких подключений, активировать параметр "Сохранить пароль".

4. При импорте сертификата пользователя необходимо предъявлять закрытый ключ, который был получен с импортируемым сертификатом. В противном случае попытки установления соединения завершатся ошибкой "Неверный пароль ключевого контейнера, или сертификат пользователя не соответствует ключу".

5. Возможны ошибки в работе параметра "Постоянное соединение" настроек VPN.

6. При установлении соединения с защищаемым ресурсом в режиме TLS после выбора сертификата, ввода пароля и/или выбора уровня доверия для доступа к ресурсу необходимо самостоятельно вернуться в веб-браузер.

7. В случае возникновения ошибки множественного подключения при установлении соединения с СД может появиться сообщение "Ошибка аутентификации пользователя. Причина: { Ошибка входа в систему }".

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