

АО «СИГНАЛ-КОМ»

УТВЕРЖДЕНО
ШКНР.00051-01 34 04-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
SIGNAL-COM CLOUD DSS
Версия 1.1

SIGNAL-COM CLOUD DSS CLIENT
Руководство пользователя

ШКНР.00051-01 34 04
Листов 22

АННОТАЦИЯ

Настоящий документ содержит руководство пользователя программного компонента Signal-COM Cloud DSS Client, предоставляющего другим приложениям стандартный программный интерфейс для защищенного взаимодействия с серверной частью программно-аппаратного комплекса Signal-COM Cloud DSS, предназначенного для централизованного хранения и дистанционного применения ключей электронной подписи.

СОДЕРЖАНИЕ

| | |
|---|----|
| Аннотация | 2 |
| Содержание | 3 |
| 1. Назначение программы | 4 |
| 1.1. Список сокращений | 4 |
| 1.2. Термины и определения | 4 |
| 2. Условия выполнения программы | 5 |
| 2.1. Требования к окружению | 5 |
| 2.2. Установка программы | 5 |
| 2.3. Удаление программы | 8 |
| 3. Выполнение программы | 10 |
| 3.1. Программа конфигурации | 10 |
| 3.2. Запуск программы | 10 |
| 3.3. Мастер создания конфигурации | 10 |
| 3.4. Изменение параметров конфигурации | 17 |
| 3.4.1. Работа со списком серверов | 17 |
| 3.4.2. Сохранение параметров конфигурации | 18 |
| 3.5. Экспорт конфигурации | 18 |
| 3.6. Импорт конфигурации | 18 |
| 4. Сообщения оператору | 20 |
| 4.1. Сообщения в программе конфигурации | 20 |
| 4.2. Сообщения в журнале событий | 21 |
| Литература | 22 |

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программно-аппаратный комплекс Signal-COM Cloud DSS предназначен для централизованного хранения и дистанционного применения ключей электронной подписи [1].

Программный компонент Signal-COM Cloud DSS Client предоставляет другим приложениям стандартный программный интерфейс для защищенного взаимодействия с серверной частью программно-аппаратного комплекса Signal-COM Cloud DSS и выполнения следующих функций:

- выбор удостоверяющего центра ПАК Signal-COM Cloud DSS для выпуска сертификата ключа проверки электронной подписи;
- выбор шаблона для формирования запроса на создание сертификата ключа проверки электронной подписи;
- генерация ключа электронной подписи и ключа проверки электронной подписи;
- формирование запроса на создание сертификата ключа проверки электронной подписи;
- отправка запроса на создание сертификата ключа проверки электронной подписи в удостоверяющий центр ПАК Signal-COM Cloud DSS;
- получение выпущенного удостоверяющим центром ПАК Signal-COM Cloud DSS сертификата ключа проверки электронной подписи;
- обновление действующего сертификата ключа проверки электронной подписи;
- отправка в ПАК Signal-COM Cloud DSS сертификата ключа проверки электронной подписи, выпущенного сторонним удостоверяющим центром;
- получение списков ключей проверки электронной подписи и сертификатов ключей проверки электронной подписи;
- создание электронной подписи для документа.

1.1. Список сокращений

В настоящем руководстве используются следующие сокращения:

- ПАК – программно-аппаратный комплекс;
- ПЭВМ – персональная электронно-вычислительная машина;
- УЦ – удостоверяющий центр;
- ЭП – электронная подпись;
- OTP - One-Time Password;
- SMS - Short Message Service;
- TCP - Transmission Control Protocol;
- TLS - Transport Layer Security;
- URL - Uniform Resource Locator.

1.2. Термины и определения

В настоящем руководстве используются следующие термины:

- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;
- сертификат ключа проверки электронной подписи – документ в электронном виде или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;
- электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к окружению

Signal-COM Cloud DSS Client поставляется для следующих операционных систем (в скобках указаны аппаратные платформы):

- Windows 8.1/10/11 (x86, x86_64);
- Windows Server 2008 R2/2012/2012 R2/2016/2019/2022 (x86_64).

Компонент Signal-COM Cloud DSS Client должен иметь доступ по протоколу TCP к адресу и порту сервера подписи (и сервера идентификации [2], если он размещается на отдельном сервере).

2.2. Установка программы

Для установки компонента Signal-COM Cloud DSS Client выполните следующие действия:

- 1) Запустите программу установки, для этого дважды щелкните мышью на файле из дистрибутива SCDSSCLIENT-X64-RUS.MSI (для 64-битных ОС) или SCDSSCLIENT-X86-RUS.MSI (для 32-битных ОС) и нажмите «Далее» (см. Рисунок 1).

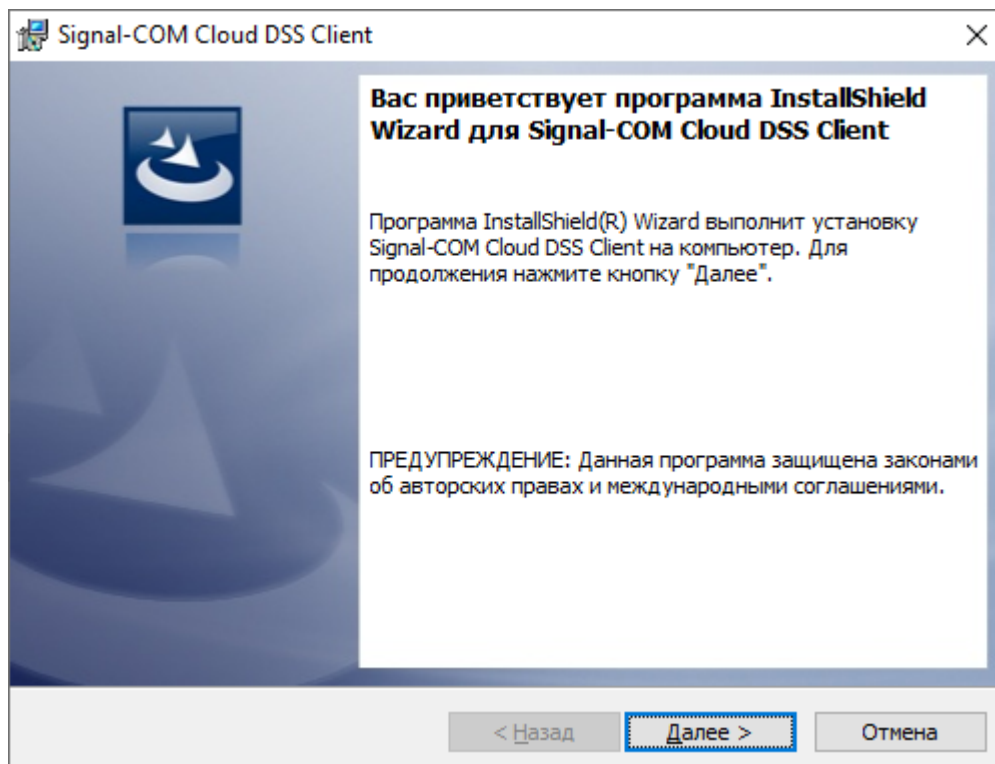


Рисунок 1

- 2) Прочитайте лицензионное соглашение и, в случае согласия, нажмите «Я принимаю условия лицензионного соглашения», затем нажмите «Далее» (см. Рисунок 2).

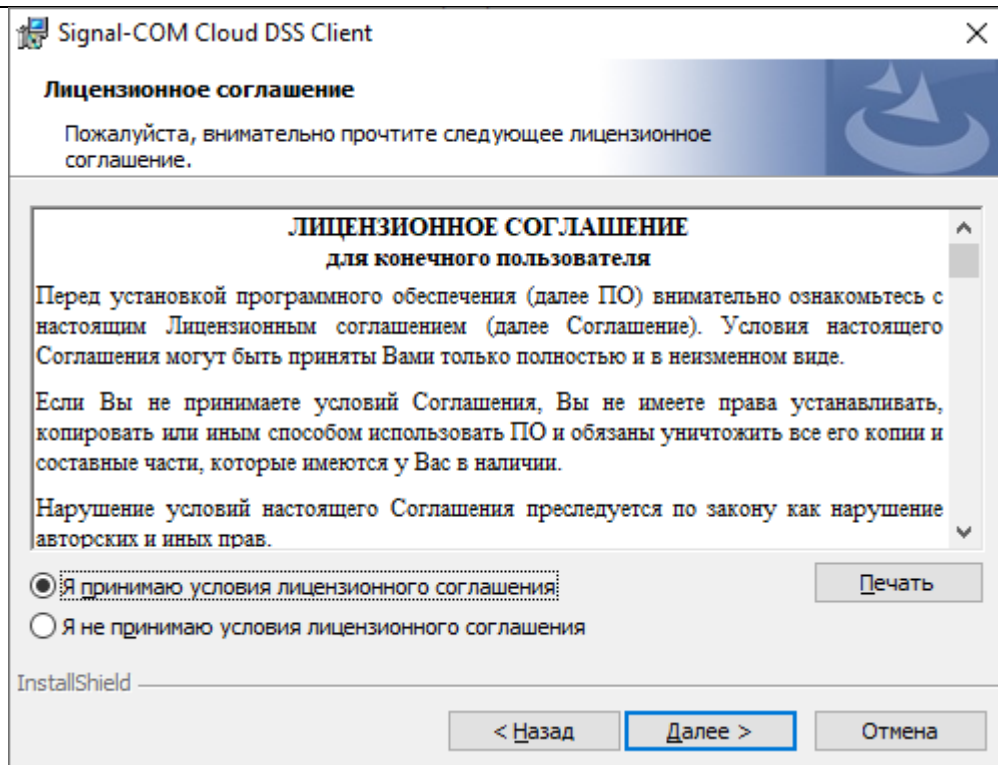


Рисунок 2

- 3) Нажмите «Установить» (см. Рисунок 3).

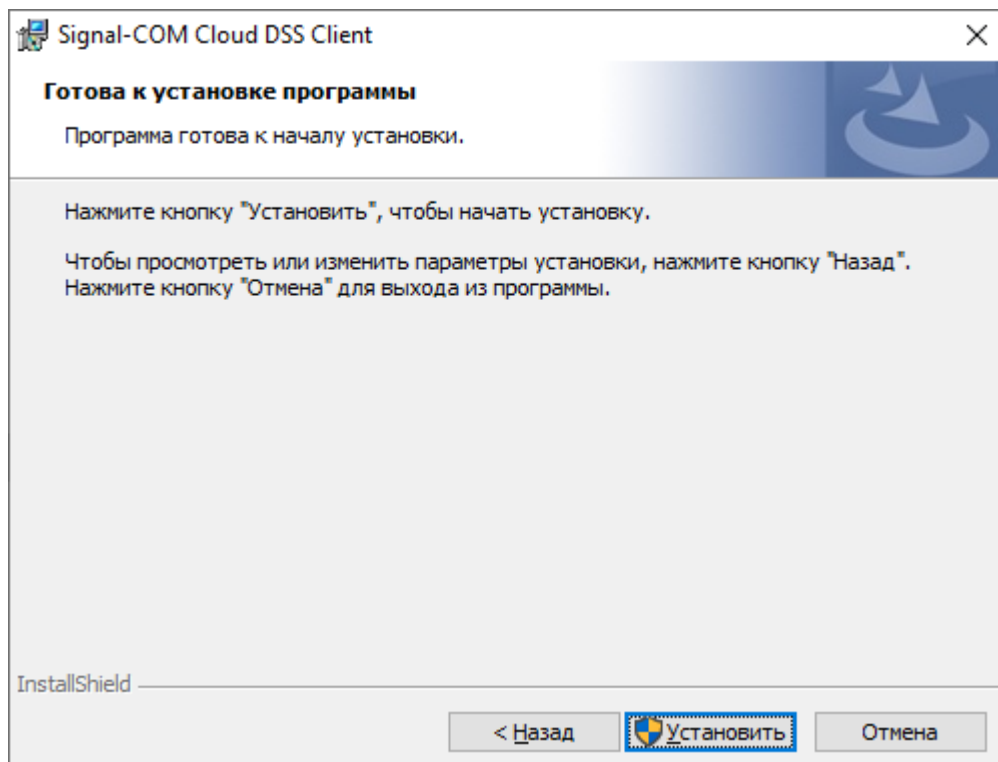


Рисунок 3

- 4) В окне контроля учетных записей убедитесь в корректности цифровой подписи разработчика программы и нажмите «Да» (см. Рисунок 4).

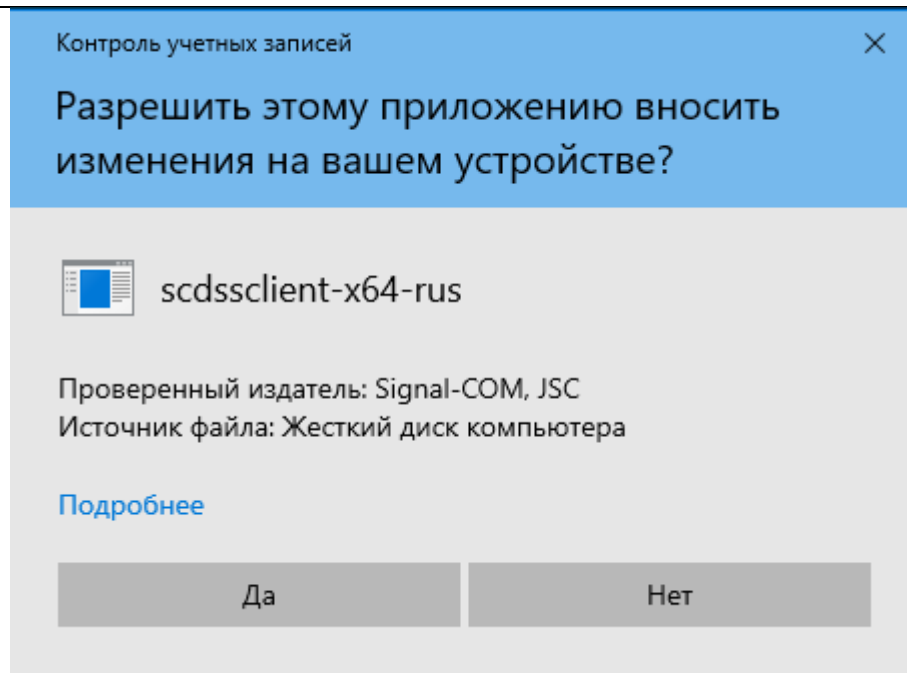


Рисунок 4

- 5) В случае успешного завершения, программа установки предложит загрузить программу конфигурации компонента Signal-COM Cloud DSS Client. Если Вы планируете настраивать Signal-COM Cloud DSS Client позднее, отключите флажок «Загрузить Signal-COM Cloud DSS Client». Для завершения программы установки нажмите «Готово» (см. Рисунок 5).

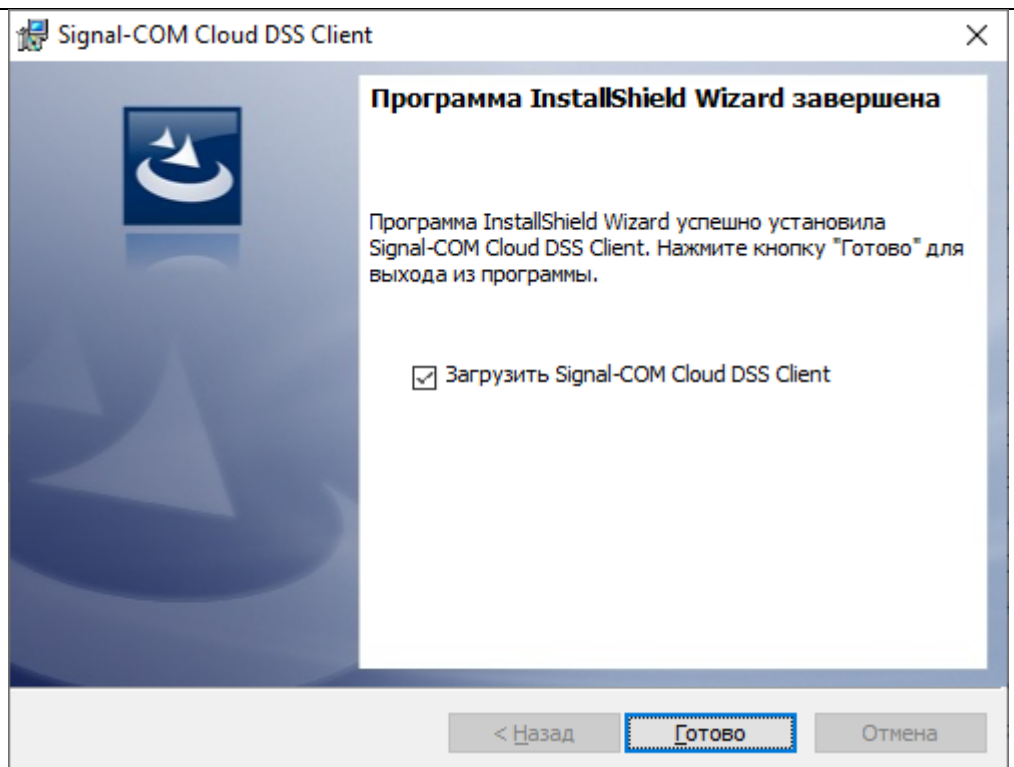


Рисунок 5

2.3. Удаление программы

Удаление компонента Signal-COM Cloud DSS Client на ОС Windows осуществляется с помощью сервиса «Программы и компоненты» панели управления ОС Windows или с помощью сервиса «Приложения и Возможности», доступного из настроек ОС Windows 10.

Для удаления выберите в списке приложение «Signal-COM Cloud DSS Client» и нажмите кнопку (меню) «Удалить». Конфигурация пользователя при удалении Signal-COM Cloud DSS Client в этом случае не удаляется.

Если вместе с компонентом Signal-COM Cloud DSS Client требуется удалить конфигурацию пользователя, выберите кнопку (меню) «Изменить». В окне «Обслуживание программ» необходимо выбрать режим «Удалить», затем в окне «Удаление программ» необходимо установить флажок «Удалить конфигурацию» (см. Рисунок 6).

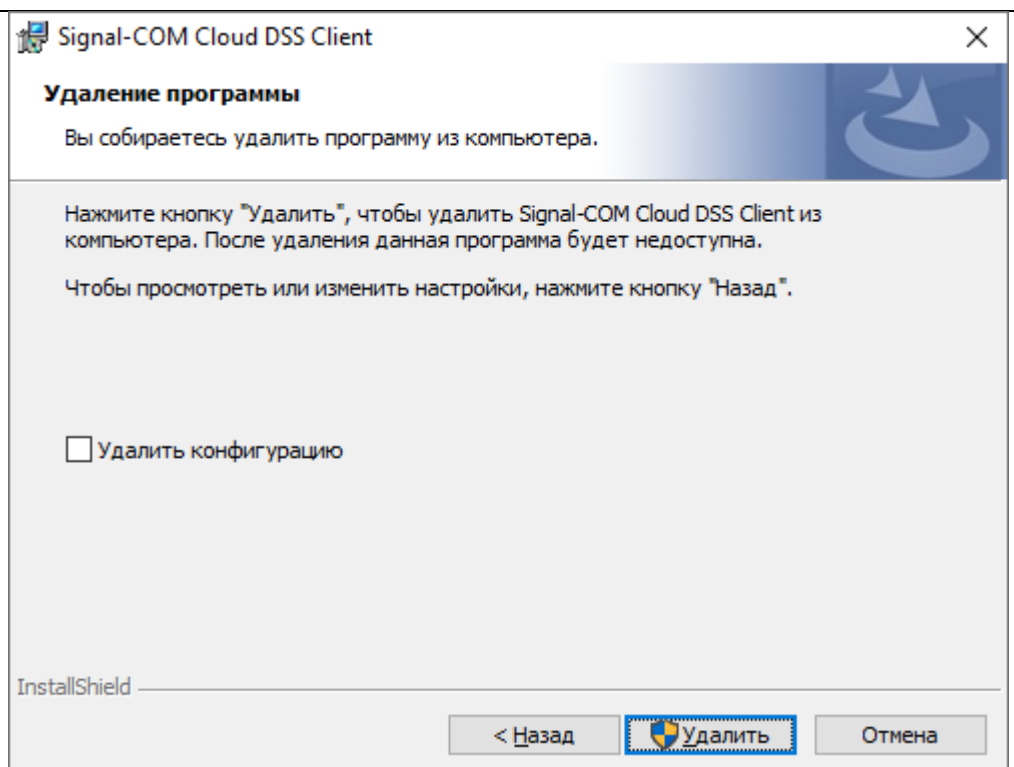


Рисунок 6

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Программа конфигурации

Программа конфигурации предназначена для настройки с помощью графического интерфейса параметров компонента Signal-COM Cloud DSS Client, необходимых для работы с серверной частью ПАК Signal-COM Cloud DSS.

Предварительная настройка Signal-COM Cloud DSS Client является обязательным условием успешной работы программных продуктов (например, Signal-COM CSP), использующих компонент для взаимодействия с ПАК Signal-COM Cloud DSS.

3.2. Запуск программы

Первый запуск программы конфигурации может быть выполнен автоматически из программы установки компонента Signal-COM Cloud DSS Client (см. п. 2.2).

В дальнейшем для запуска программы конфигурации необходимо использовать меню программ операционной системы («Signal-COM Cloud DSS Client»).

3.3. Мастер создания конфигурации

При запуске программа конфигурации проверяет наличие файла конфигурации Signal-COM Cloud DSS Client на ПЭВМ пользователя. В случае отсутствия файла конфигурации выполняется мастер создания конфигурации, позволяющий последовательно, по шагам, задать все необходимые для работы Signal-COM Cloud DSS Client параметры.

Работа мастера может быть прервана в любой момент без сохранения созданной конфигурации с помощью кнопки «Отмена». После прерывания и завершения работы программа конфигурации может быть запущена вновь «с нуля» в любой удобный момент времени (см. п. 3.2).

Для ускорения процедуры настройки мастер создания конфигурации позволяет импортировать файл архива конфигурации Signal-COM Cloud DSS Client, сформированный с помощью процедуры экспорта конфигурации (см. п. 3.5).

Для импорта конфигурации необходимо в окне «Импорт конфигурации» установить флажок «Импортировать» и задать соответствующий файл архива конфигурации (см. Рисунок 7). Нажмите «Далее».

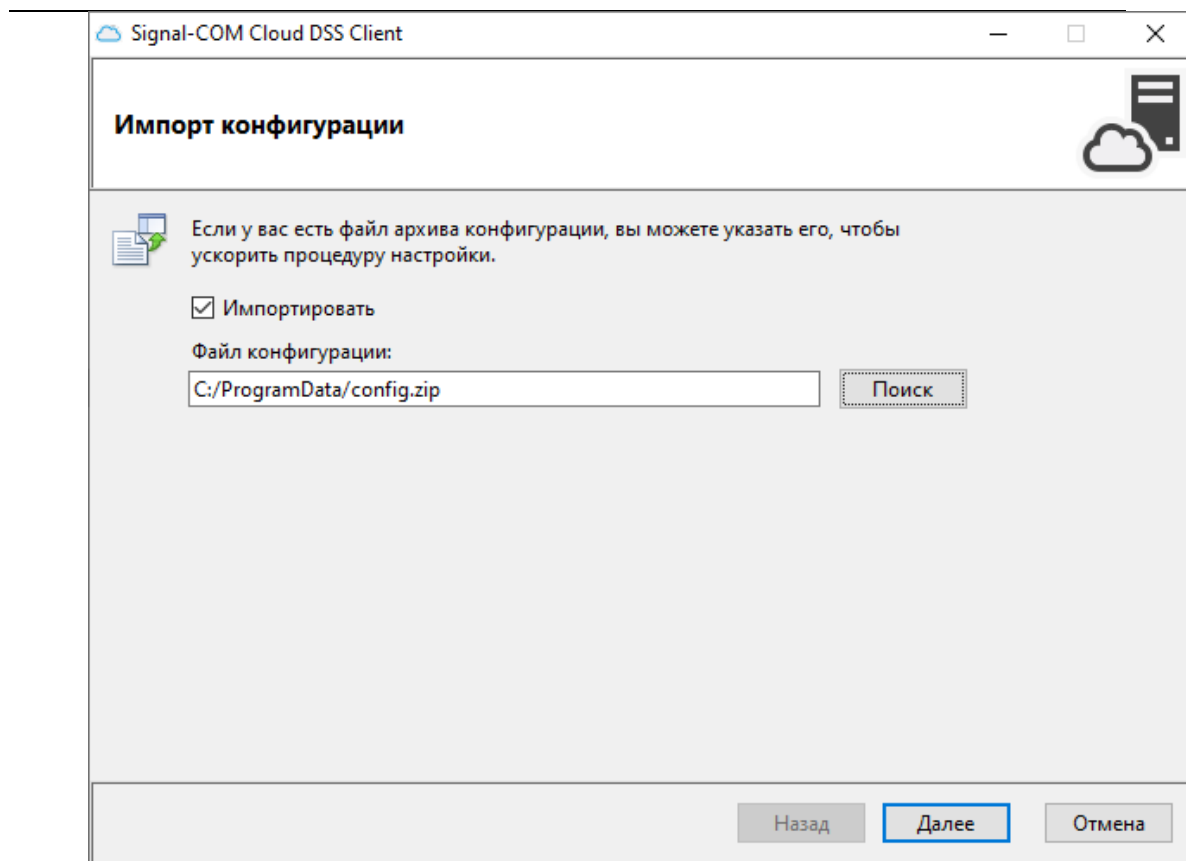


Рисунок 7

В случае успешного импорта конфигурации Вам будет предложено завершить работу мастера.

Для завершения настройки Signal-COM Cloud DSS Client нажмите «Да»: конфигурация будет сохранена, и работа мастера завершена.

Если Вам требуется продолжить настройку конфигурации, нажмите «Нет».

В окне «Журнал» (см. Рисунок 8) можно включить ведение журнала событий. Журнал событий может потребоваться для детальной диагностики ошибки, возникшей на последнем шаге мастера создания конфигурации или в процессе эксплуатации программных продуктов (например, Signal-COM CSP), использующих Signal-COM Cloud DSS Client.

В случае возникновения ошибки в окне «Параметры выпуска сертификата», Вы можете вернуться в окно «Журнал» с помощью кнопки «Назад» и включить ведение журнала событий.

Для включения ведения журнала событий (см. п. 4.2) выполните следующие действия:

- установите флажок «Вести журнал»;
- задайте каталог и имя файла журнала;
- задайте уровень детализации журнала событий.

Параметр «Уровень детализации» может принимать следующие значения:

- «Ошибка» – выводятся только сообщения об ошибках;
- «Предупреждение» – дополнительно к сообщениям уровня «Ошибка» выводятся сообщения с предупреждениями;
- «Отладка» – дополнительно к сообщениям «Предупреждение» выводятся отладочные сообщения;
- «Трассировка» – дополнительно к сообщениям «Отладка» выводятся трассировочные сообщения.

Для детальной диагностики ошибки можно задать любой уровень детализации.

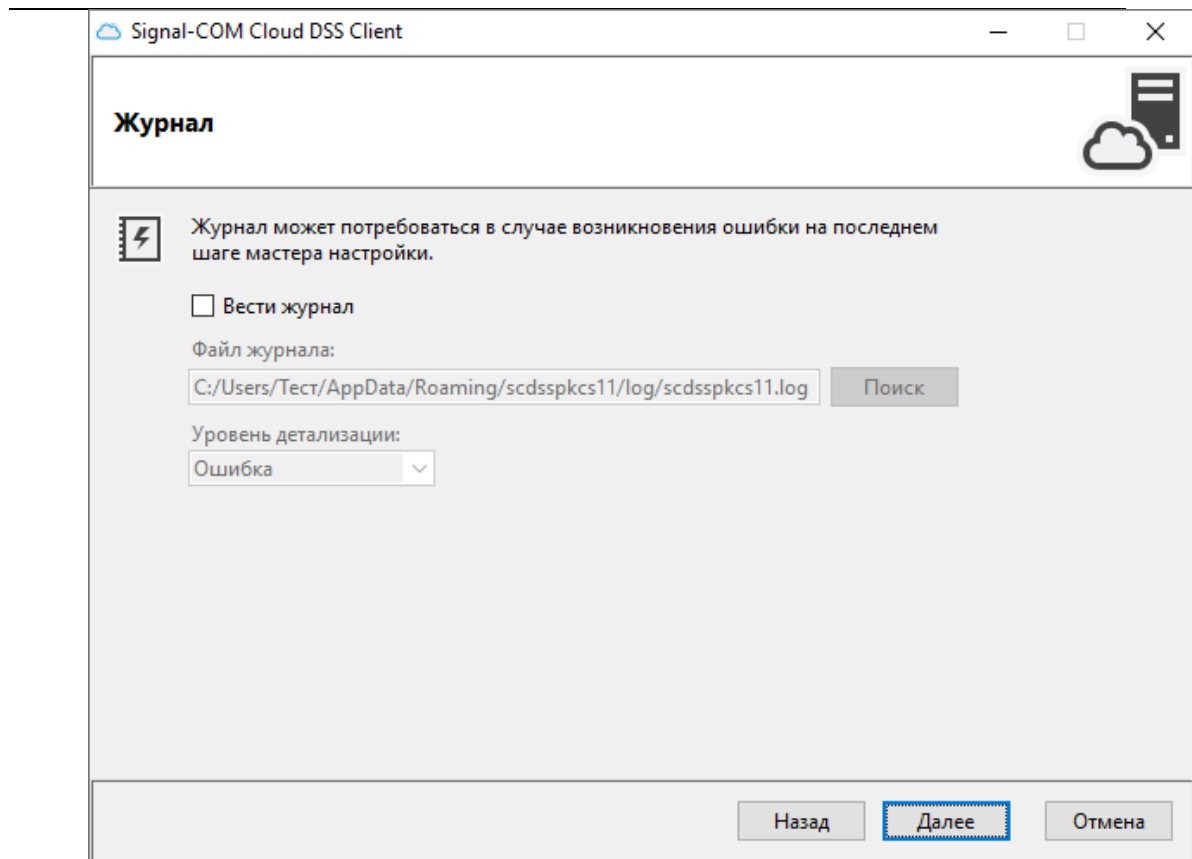


Рисунок 8

Если для защищенного взаимодействия с сервером ПАК Signal-COM Cloud DSS (по протоколу TLS) требуется использование российских криптографических алгоритмов, в окне «Параметры протокола TLS» установите флажок «Использовать российские алгоритмы в TLS» (см. Рисунок 9).

Если флажок «Использовать российские алгоритмы в TLS» установлен, необходимо задать путь к ключевому контейнеру СКЗИ «Крипто-КОМ». Вы можете задать путь к уже существующему ключевому контейнеру или указать путь для создания нового ключевого контейнера. Нажмите «Далее».

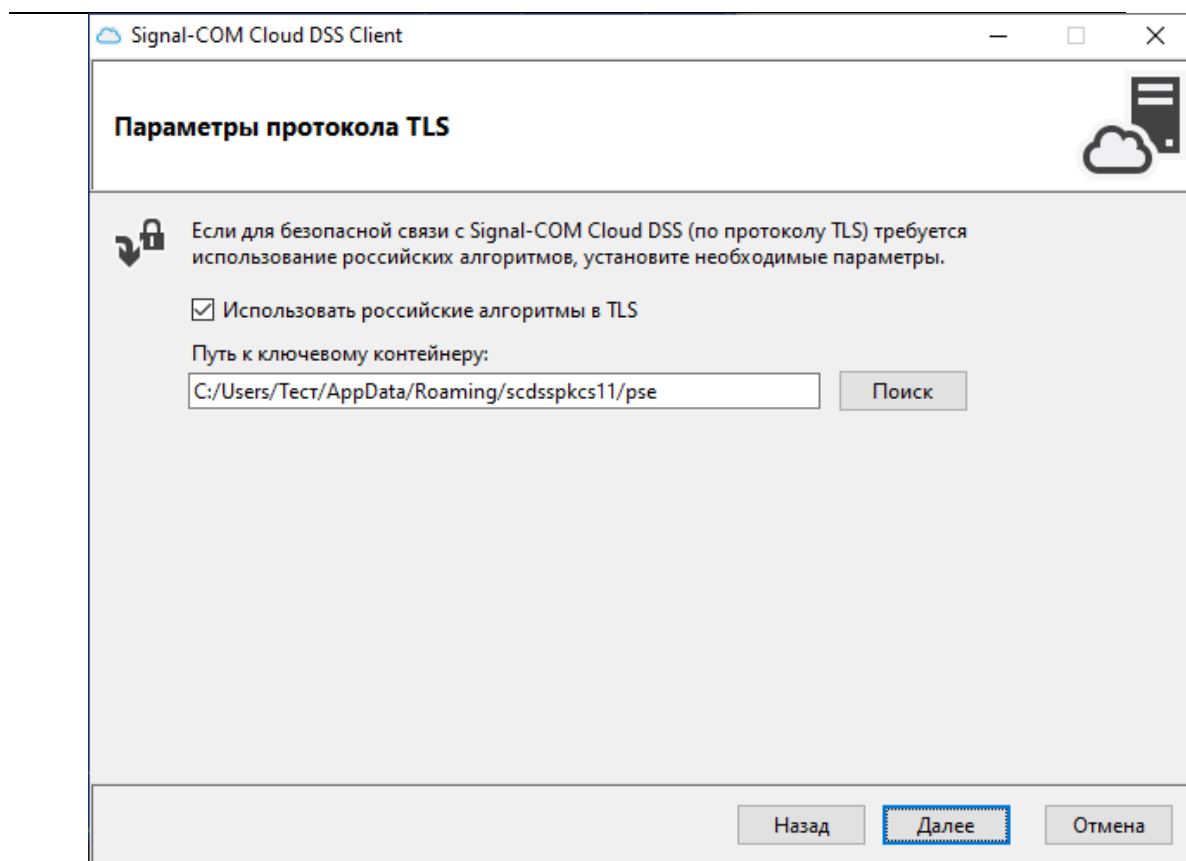


Рисунок 9

Если заданного ключевого контейнера не существует, перед его созданием выполняется процедура инициализации генератора случайных чисел, которая предполагает интерактивное взаимодействие с пользователем (см. Рисунок 10).



Рисунок 10

В окне «Параметры Signal-COM Cloud DSS» необходимо задать следующие параметры: имя, URL-адрес сервера подписи (если порт сервера отличается от номера 443, необходимо задать номер порта в конце доменного имени после двоеточия), сертификат удостоверяющего центра сервера подписи и Ваш логин. Если сервер идентификации [2] размещается на отдельном

сервере, необходимо также задать URL-адрес и сертификат УЦ этого сервера (см. Рисунок 11). Нажмите «Далее».

Signal-COM Cloud DSS Client

Параметры Signal-COM Cloud DSS

Задайте параметры сервера подписи и сервера идентификации.

Параметры сервера подписи

Имя: Тестовый сервер

Адрес (URL): https://dss-ws.signal-com.ru

Сертификат УЦ: C:/Users/Тест/AppData/Roaming/scdsspkcs11/CA/DSS1/cacert.cer Поиск

Параметры сервера идентификации

Логин: test

☒ размещен на том же сервере, что и сервер подписи

Адрес (URL):

Сертификат УЦ: Поиск

Назад Далее Отмена

Рисунок 11

Окно «Параметры выпуска сертификата» (см. Рисунок 14) предназначено в первую очередь для контроля правильности настройки параметров сервера ПАК Signal-COM Cloud DSS, заданных на предыдущих шагах мастера создания конфигурации.

При переходе к окну «Параметры выпуска сертификата» (см. Рисунок 14) программа конфигурации осуществляет взаимодействие с сервером ПАК Signal-COM Cloud DSS.

Задайте в соответствующем окне логин и пароль для доступа к ПАК Signal-COM Cloud DSS (см. Рисунок 12).

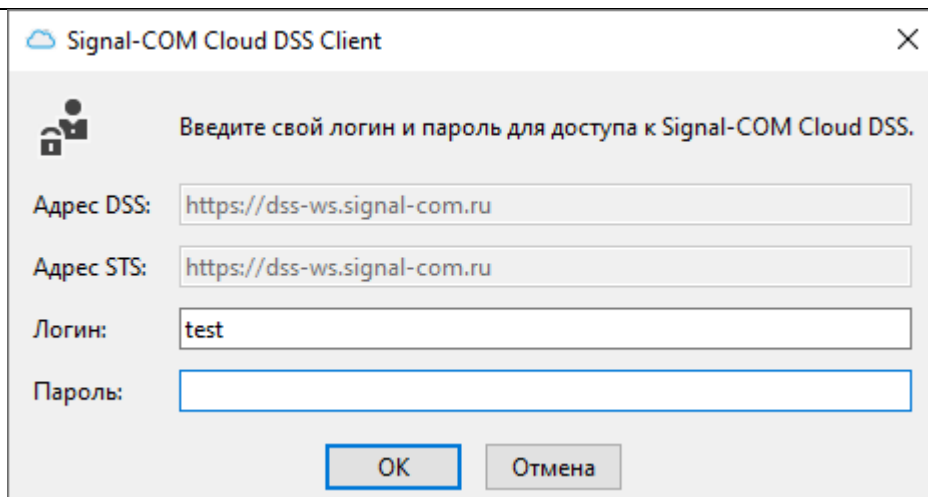


Рисунок 12

Если для входа в систему требуется двухфакторная аутентификация, введите в соответствующем окне полученный по каналу второго фактора код подтверждения операции входа в систему (например, в SMS). Если для вторичной аутентификации используется приложение MobileDSS, подтвердите операцию входа в систему в приложении MobileDSS, затем в окне программы конфигурации нажмите «OK» (см. Рисунок 13).

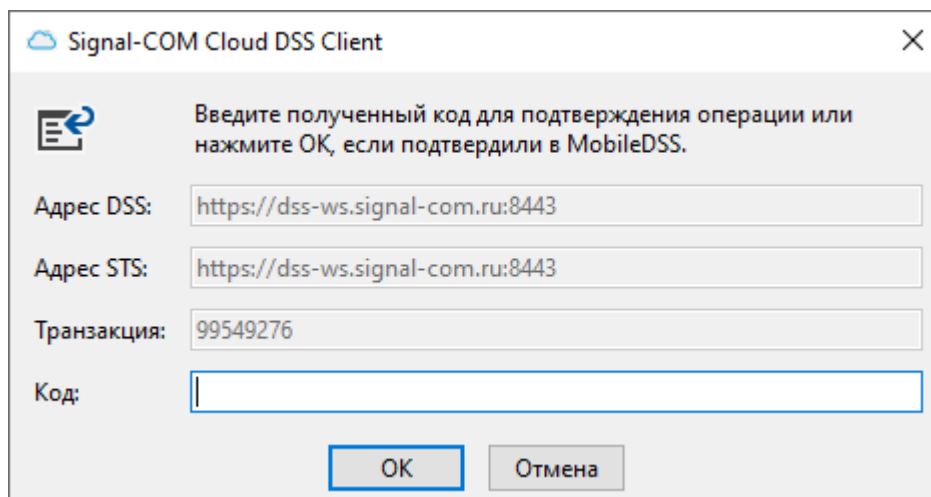


Рисунок 13

Если соединение с сервером ПАК Signal-COM Cloud DSS по каким-то причинам установить не удалось, будет выдано соответствующее сообщение об ошибке (см. п. 4.1). В этом случае рекомендуется включить журнал событий. Для этого необходимо вернуться в окно «Журнал» с помощью кнопки «Назад» и включить ведение журнала событий (см. Рисунок 8). После включения журнала событий необходимо вновь перейти к окну «Параметры выпуска сертификата» для повторения ошибочной ситуации. В журнал событий будет записана детальная информация об ошибке.

Если параметры сервера ПАК Signal-COM Cloud DSS на предыдущих шагах были заданы корректно, в окне «Параметры выпуска сертификата» будет доступен для редактирования флажок «Использовать УЦ Signal-COM Cloud DSS», а также доступна кнопка «Готово» (см. Рисунок 14).

В окне «Параметры выпуска сертификата» можно дополнительно настроить параметры выпуска сертификата, которые будут использоваться в приложениях при создании ключей ЭП.

Примечание. В самой программе конфигурации ключи ЭП не создаются.

Настройка параметров выпуска сертификата для существующих программных продуктов, использующих Signal-COM Cloud DSS Client (например, Signal-COM CSP), является

необязательной. Эти продукты используют собственный графический интерфейс пользователя для задания параметров выпуска сертификата при создании ключей ЭП.

По умолчанию флажок «Использовать УЦ Signal-COM Cloud DSS» установлен. Это значит, что при создании ключей ЭП в ПАК Signal-COM Cloud DSS, запрос на создание сертификата ключа проверки ЭП будет отправлен в заданный удостоверяющий центр.

При задании переключателя «Создать новый сертификат» необходимо выбрать из списка требуемые удостоверяющий центр и шаблон запроса на сертификат ключа проверки ЭП.

Signal-COM Cloud DSS Client

Параметры выпуска сертификата

Если для выпуска сертификата Вы используете Удостоверяющий центр Signal-COM Cloud DSS, задайте его параметры.

☒ Использовать УЦ Signal-COM Cloud DSS

☒ Создать новый сертификат

Удостоверяющий центр: e-Notary Test CA

Шаблон запроса сертификата: Шаблон для физических лиц

☐ Обновить сертификат

Ключевой контейнер:

Назад Готово Отмена

Рисунок 14

Если у Вас уже имеется действующий сертификат, выпущенный УЦ ПАК Signal-COM Cloud DSS, Вы можете обновить его, выбрав переключатель «Обновить сертификат» и задав соответствующий ключевой контейнер (см. Рисунок 15).

При обновлении сертификата задание удостоверяющего центра и шаблона на создание сертификата ключа проверки ЭП не требуется, в этом случае используются параметры, которые были заданы для выпуска обновляемого сертификата.

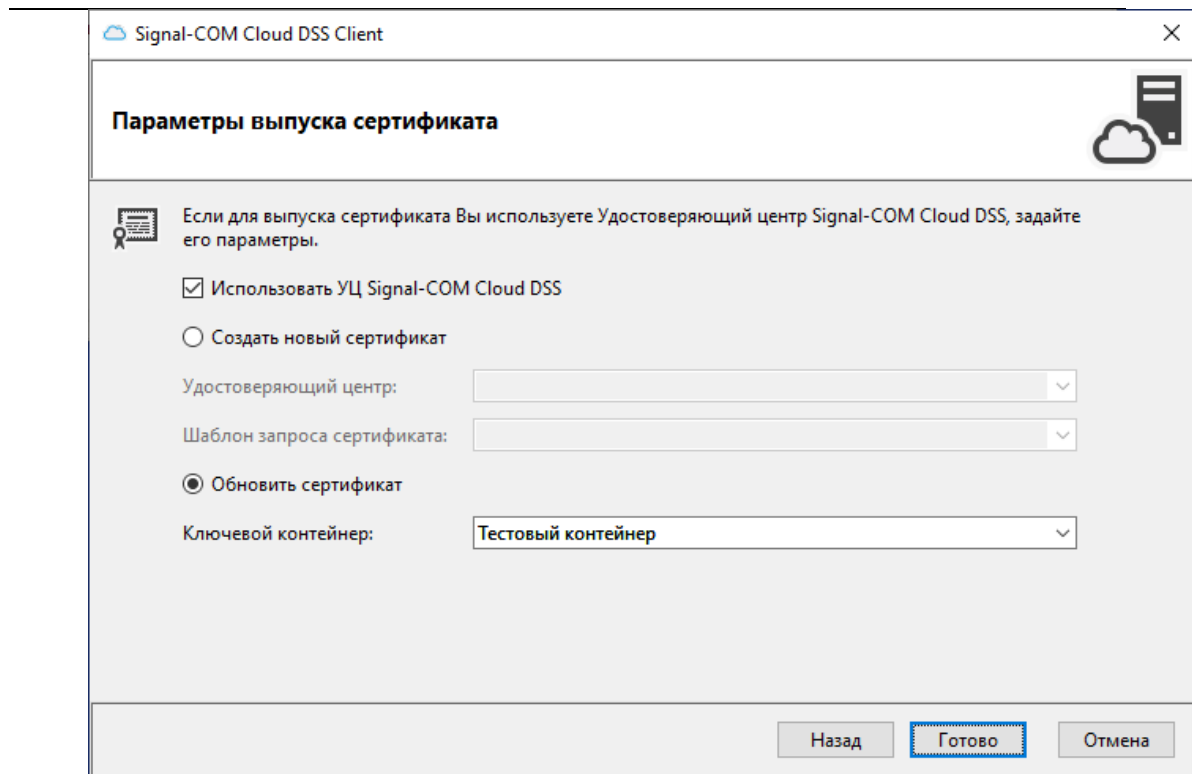


Рисунок 15

Если для выпуска Вашего сертификата Вы планируете использовать сторонний удостоверяющий центр, флажок «Использовать УЦ Signal-COM Cloud DSS» необходимо отключить.

Для завершения настройки Signal-COM Cloud DSS Client нажмите «Готово».

Конфигурация будет сохранена, и работа мастера завершена.

3.4. Изменение параметров конфигурации

Параметры конфигурации компонента Signal-COM Cloud DSS Client, созданной с помощью мастера создания конфигурации (см. п. 3.3), могут быть изменены при последующих запусках программы конфигурации (мастер создания конфигурации в этом случае не используется).

В частности, можно выполнить действия, которые не доступны в мастере создания конфигурации: добавить в конфигурацию параметры других серверов ПАК Signal-COM Cloud DSS (см. п. 3.4.1).

3.4.1. Работа со списком серверов

Для работы со списком серверов ПАК Signal-COM Cloud DSS выполните следующие действия:

- запустите программу конфигурации (см. п. 3.2);
- выберите вкладку «Серверы» (см. Рисунок 16).

Если необходимо задать параметры нового сервера ПАК Signal-COM Cloud DSS, выполните следующие действия:

- нажмите «Добавить»;
- задайте параметры нового сервера в окне «Параметры Signal-COM Cloud DSS», нажмите «Далее» (см. Рисунок 11);
- в окне «Параметры выпуска сертификата» задайте параметры выпуска сертификата, нажмите «Готово» (см. Рисунок 14).

Для изменения параметров сервера ПАК Signal-COM Cloud DSS выполните следующие действия:

- выберите требуемый сервер в списке;

- нажмите «Изменить»;
- если требуется, измените параметры сервера в окне «Параметры Signal-COM Cloud DSS», нажмите «Далее» (см. Рисунок 11);
- если требуется, измените параметры выпуска сертификата в окне «Параметры выпуска сертификата», нажмите «Готово» (см. Рисунок 14).

Если необходимо удалить параметры сервера ПАК Signal-COM Cloud DSS из конфигурации, выполните следующие действия:

- выберите требуемый сервер в списке;
- нажмите «Удалить».

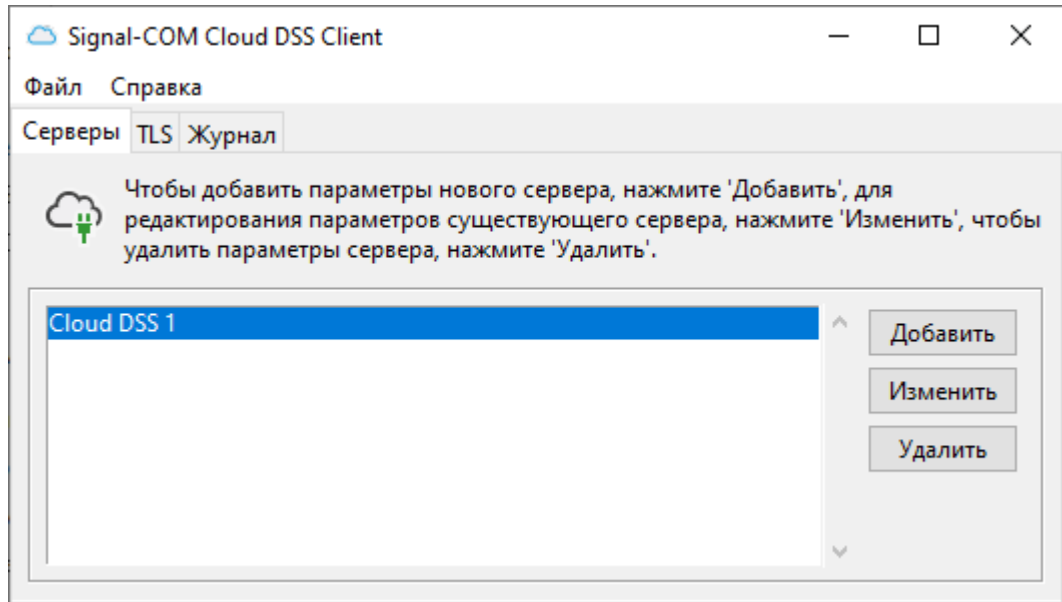


Рисунок 16

3.4.2. Сохранение параметров конфигурации

Изменения, внесенные в программе конфигурации, сохраняются в памяти программы.

Для того чтобы внесенные изменения стали доступны компоненту Signal-COM Cloud DSS Client, необходимо сохранить их в файле конфигурации. Для этого необходимо выполнить одно из следующих действий:

- выбрать пункт меню программы конфигурации «Файл» -> «Сохранить»;
- нажать комбинацию клавиш Ctrl+S;
- нажать «Да» в окне с сообщением «Вы хотите сохранить внесенные изменения?» при выходе из программы.

3.5. Экспорт конфигурации

При экспорте конфигурации формируется файл архива, включающего необходимые файлы конфигурации Signal-COM Cloud DSS Client.

Для экспорта конфигурации необходимо выполнить следующие действия:

- выбрать пункт меню программы конфигурации «Файл» -> «Экспорт...» или нажать комбинацию клавиш Ctrl+C;
- в окне «Экспорт конфигурации» задать имя файла архива конфигурации.

3.6. Импорт конфигурации

При импорте конфигурации используется файл архива, сформированный с помощью процедуры экспорта (см. п. 3.5).

Для импорта конфигурации необходимо выполнить следующие действия:

- выбрать пункт меню программы конфигурации «Файл» -> «Импорт...» или нажать комбинацию клавиш Ctrl+O;
- в окне «Импорт конфигурации» выбрать файл архива конфигурации;

- нажать «Да» в окне с сообщением «Текущая конфигурация будет перезаписана. Продолжить?».

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Сообщения в программе конфигурации

Сообщения программы конфигурации оператору (пользователю) реализованы в виде модальных диалогов, которые отображаются для оповещения оператора об ошибках в программе или для привлечения внимания перед выполнением некоторых действий (см. Таблица 1).

Таблица 1

| Сообщение | Описание |
|--|--|
| Адрес сервера подписи не задан. | Не задан URL-адрес сервера подписи. |
| Сертификат УЦ сервера подписи не задан. | Не задан путь к файлу сертификата УЦ сервера подписи. |
| Файл сертификата УЦ сервера подписи не найден. | Заданный файл сертификата УЦ сервера подписи не найден. |
| Адрес сервера идентификации не задан. | Не задан URL-адрес сервера идентификации [2]. |
| Сертификат УЦ сервера идентификации не задан. | Не задан путь к файлу сертификата УЦ сервера идентификации. |
| Файл сертификата УЦ сервера идентификации не найден. | Заданный файл сертификата УЦ сервера идентификации не найден. |
| Вы уверены, что хотите удалить запись 'Cloud DSS 1'? | Данное предупреждение выдается для подтверждения удаления параметров сервера ПАК Signal-COM Cloud DSS. |
| Настройка еще не завершена. Прервать работу мастера? | Данное предупреждение выдается для подтверждения преждевременного завершения мастера создания конфигурации. |
| При создании ключевого контейнера произошла ошибка. | Произошла ошибка при создании ключевого контейнера. Код ошибки необходимо сообщить службе поддержки. |
| Файл библиотеки не задан. | Не задан путь к файлу криптографической библиотеки. |
| Файл библиотеки не найден. | Заданный файл криптографической библиотеки не найден. |
| Путь к ключевому контейнеру не задан. | Путь к каталогу ключевого контейнера не задан. |
| Выполнение операции прервано пользователем. | Пользователь прервал выполнение операции в одном из окон диалога, нажав «Отмена» или закрыв окно. |
| Неверный логин или пароль. | В окне диалога введен неверный логин или пароль для доступа к ПАК Signal-COM Cloud DSS. |
| Неверный код OTP. | Введенный в окне диалога код OTP отличается от кода, полученного по каналу вторичной аутентификации. |
| Произошла коммуникационная ошибка. | Невозможно установить соединение с сервером ПАК Signal-COM Cloud DSS. Возможно, неверно задан URL-адрес сервера подписи или сервера идентификации. |

| Сообщение | Описание |
|--|--|
| Истек коммуникационный тайм-аут. | Истек тайм-аут при установлении соединения или передаче данных. Возможно, неверно задан URL-адрес сервера подписи или сервера идентификации. |
| Произошла ошибка протокола SSL. | Произошла ошибка при установлении защищенного соединения. Возможно, задан некорректный файл сертификата УЦ сервера подписи или сервера идентификации. Возможно, в конфигурации отключен флаг «Использовать российские алгоритмы в TLS», а на сервере ПАК Signal-COM Cloud DSS используются российские алгоритмы. |
| При получении данных с сервера произошла ошибка. | Произошла ошибка при взаимодействии с сервером ПАК Signal-COM Cloud DSS. Код ошибки необходимо сообщить службе поддержки. |
| Файл журнала не задан. | Не задан файл журнала событий. |
| Каталог журнала не существует. Вы хотите создать его? | Данное сообщение выдается для подтверждения создания заданного каталога журнала событий, если каталог не существует. |
| Переменная окружения 'OPENSSL_CONF' не задана. | Обратитесь в службу поддержки. |
| Файл конфигурации OpenSSL не найден. | Обратитесь в службу поддержки. |
| При выполнении приложения произошла непредвиденная ошибка. Обратитесь к разработчику приложения. | Обратитесь в службу поддержки. |
| При записи конфигурации произошла ошибка. | Возможно, у Вас нет прав на запись в файл конфигурации. Обратитесь в службу поддержки. |
| Вы хотите сохранить внесенные изменения? | Данное сообщение выдается для подтверждения сохранения изменений в файле конфигурации. |

4.2. Сообщения в журнале событий

Сообщения оператору (пользователю) в журнале событий предназначены для выявления проблем при взаимодействии компонента Signal-COM Cloud DSS Client с серверной частью ПАК Signal-COM Cloud DSS.

По умолчанию журнал событий не ведется.

Для настройки журнала событий необходимо использовать программу конфигурации (см. п. 3.3).

ЛИТЕРАТУРА

1. Signal-COM Cloud DSS. Описание применения. ШКНР.00051-01 31 01. АО «СИГНАЛ-КОМ», 2021.
2. OASIS Standard, WS-Trust 1.3, 19 March 2007.