



Сервер доступа

Инструкция по установке

Версия 15.3



Содержание

1. Общие сведения.....	3
1.1 Принцип авторизации пользователя без Сервера доступа	5
1.2 Принцип авторизации пользователя через Сервер доступа	5
2. Подготовка к установке Сервера доступа.....	6
2.1 Рекомендации по подготовке платформы	7
3. Установка и настройка Сервера доступа	8
3.1 Установка Сервера доступа на ОС Windows	8
3.2 Установка Сервера доступа на ОС Linux	10
3.3 Миграция Сервера доступа с ОС Windows на ОС Linux.....	17
3.4 Удаление сервиса.....	25
4. Использование провайдера шифрования OpenSSL.....	27
4.1 Получение сертификата.....	27
4.2 Подготовка сертификата	28
4.3 Настройка сервера QUIK	30
4.4 Настройка сервера доступа	34
4.5 Настройка Рабочего места QUIK для подключения по OpenSSL.....	36
4.6 Настройка подключения Web2QUIK по OpenSSL	38
4.7 Добавление цепочки сертификатов УЦ в https-сертификат web2QUIK	39
4.8 Замена истекшего сертификата	40

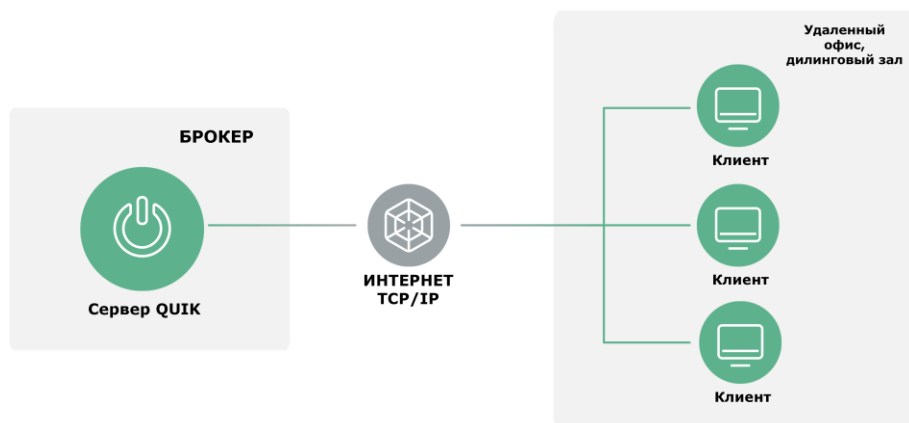
Ваши пожелания и комментарии к данной Инструкции направляйте по электронной почте на адрес: quiksupport@argatech.com



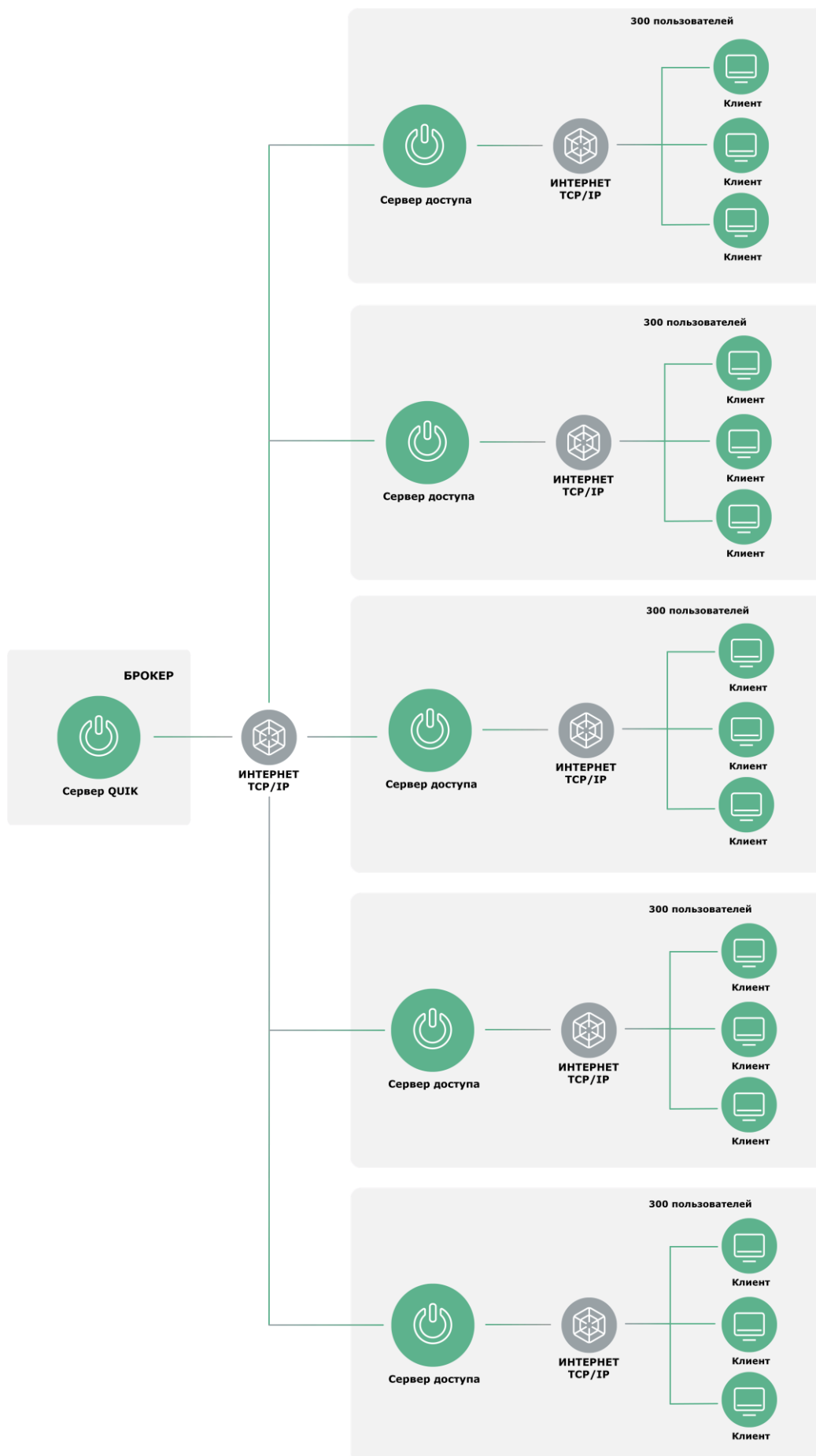
1. Общие сведения

Сервер доступа является отдельным модулем сервера системы QUIK, обслуживающим определенную группу подключенных пользователей. Он предназначен для сокращения сетевого трафика между сервером брокерской системы и группой пользователей интернет-трейдинга, а также для снижения нагрузки на основной сервер системы QUIK.

Сервер доступа рекомендуется для использования брокерам и субброкерам, имеющим число одновременных подключений клиентских терминалов более 300. Основное назначение Сервера доступа – мультипликатор и снижение нагрузки на сервер QUIK.



1. Без применения Сервера доступа трафик пропорционален количеству рабочих мест

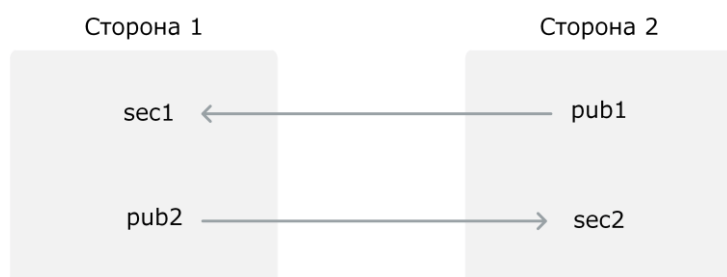


2. С сервером доступа суммарный трафик ненамного превышает величину для одного терминала.

1.1 Принцип авторизации пользователя без Сервера доступа

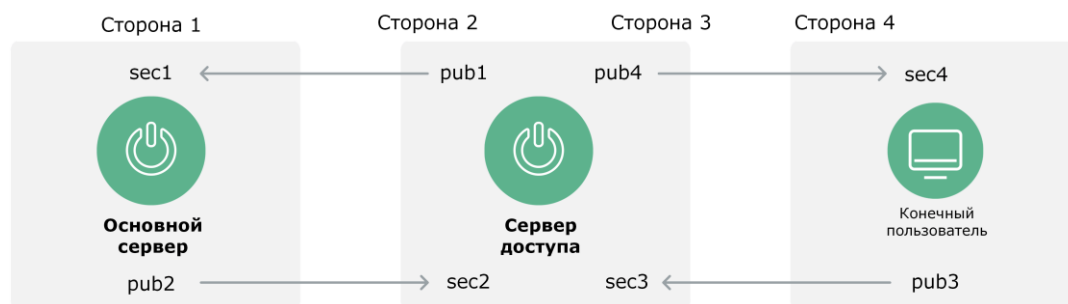
Для установления двухсторонней засекреченной связи с помощью открытого и закрытого ключа требуется два набора ключей (под одним набором понимается публичная и секретная части одного ключа).

У каждой стороны есть публичная часть ключа другой стороны. Публичная часть ключа предназначена для шифрования данных.



Расшифровать эти данные можно только секретной частью ключа, которая находится на другой стороне. Таким образом, чтобы Сторона 1 смогла принять зашифрованные данные от Стороны 2, необходимо, чтобы эти данные были зашифрованы публичной частью 1 ключа, секретная часть которого находится только у Стороны 1.

1.2 Принцип авторизации пользователя через Сервер доступа



В работе связи «Основной сервер – Сервер доступа – Конечный пользователь» участвуют четыре набора ключей:

Набор ключей	Назначение
Ключ основного сервера (sec1, pub1)	Ключ основного сервера для подключения клиентов. Секретная часть этого ключа хранится на сервере. Публичная часть раздается всем пользователям, которые



	будут заходить на основной сервер, в том числе и Серверу доступа
Ключ Сервера доступа для основного сервера (sec2, pub2)	Ключ Сервера доступа для соединения с основным сервером. Публичная часть этого ключа регистрируется на основном сервере
Ключ Сервера доступа для клиентов (sec3, pub3)	Ключ Сервера доступа для подключения клиентов. Вместо этого ключа может использоваться Ключ основного сервера
Ключ клиента (sec4, pub4)	Публичная часть ключа (pub4) хранится на основном сервере. Клиенты, подключающиеся к Серверу доступа, авторизуются на основном сервере наравне с Сервером доступа

Ключ Сервера доступа для основного сервера используется тот же, что и при подключении обычного клиентского терминала QUIK к серверу QUIK. Публичную часть этого ключа необходимо зарегистрировать в программе QUIK Administrator для пользователя, под именем которого будет заходить Сервер доступа на основной сервер. В программе QUIK Administrator в справочнике «Пользователи» в окне редактирования на вкладке «Общие права» необходимо установить признак «Сервер доступа».

В программе QUIK Administrator в справочнике «Управление серверами» (меню **Сервер QUIK/Управление серверами**) необходимо добавить пользователя, под именем которого происходит подключение Сервера доступа (необходимо для подключения программы QMonitor к серверу доступа).

2. Подготовка к установке Сервера доступа

При формировании ключей программой «KeyGen.exe» их наименования должны быть уникальны.

Пример некорректных ключей:

```
Имя ключа <Ключ Сервера доступа для основного сервера>= «SubServer»
Имя ключа <Ключ Сервера доступа для клиентов>= «Sub»
```

Ошибка в данном примере заключается в том, что наименования обоих ключей содержат слово «Sub». Если у клиентов в настройках соединения в поле «Ключ сервера» написано «Sub», система не сможет определить, на какой ключ ссылается это соединение.



Доступна схема подключения клиентов к Серверу доступа через OpenSSL.
Подробнее см. в п. 4.

Ключ Сервера доступа для клиента = Ключ основного сервера. Если необходимо обеспечить возможность клиентам подключаться на Сервер доступа с тем же публичным ключом, что и на основной сервер, то перед установкой программы «Сервер доступа» необходимо:

1. Проверить наличие следующих файлов в корневой папке основного сервера:

- **secrserv.txk** – файл, который содержит секретную часть ключа основного сервера и пароль к этому ключу.
- **quik.ini** – файл, который содержит пароль (секция [usend_module]/поле «password»).

2. Создать **Ключ Сервера доступа для основного сервера** с помощью Программы для создания и управления ключами (KeyGen).

В файле публичных ключей клиента, должен содержаться тот же Ключ основного сервера, что и в файле публичных ключей «Сервера доступа».

Схема работы:



2.1 Рекомендации по подготовке платформы

На компьютерах с серверным ПО QUIK не рекомендуется использование любого системного ПО, которое в режиме реального времени или с некоторой периодичностью анализирует данные на диске, данные, передаваемые по сети, и прочее. К такому ПО можно отнести,



например, антивирусы. Его работа может вызвать заметные проблемы с производительностью системы QUIK.

3. Установка и настройка Сервера доступа

3.1 Установка Сервера доступа на ОС Windows

1. Скопируйте секретную часть ключа основного сервера (обычно это файл `secrserv.txk` в папке основного сервера QUIK) в файл `secrserv.txk` в папке Сервера доступа (необходимо скопировать полностью файл или текст ключа текстовым редактором).
2. С помощью Программы для создания и управления ключами (KeyGen) сгенерируйте новый ключ для технологического пользователя Сервера доступа.
3. Зарегистрируйте технологического пользователя Сервера доступа в программе QUIK Administrator:
 - Внесите пользователя в справочник «Пользователи»;
 - На вкладке «Общие права» включите флажок «Сервер доступа»;
 - Присвойте ему созданные ключи доступа.Подробнее см. Руководство по администрированию QUIK Administrator п. 2.3.2.
4. Из файла `secring.txk` с новым ключом добавьте в файл `secrserv.txk` секретную часть ключа технологического пользователя Сервера доступа. На Сервере доступа в `secrserv.txk` должно быть две секции: «от Сервера доступа» и «от основного сервера».
5. Скопируйте `pubring.txk` нового ключа в папку Сервера доступа. Убедитесь, что в `pubring.txk` есть обе секции: «от Сервера доступа» и «от основного сервера».
6. Проверьте, что в файле `qcrypto.cfg` Сервера доступа указаны следующие параметры:

```
SECRING=secrserv.txk
PUBRING=quik.dwq

[auth]
look=qcrypto.cfg,db_look
look=qcrypto.cfg,locke_look

[db_look]
do=_QXKey
use=dwqx.dll
```



```
[locke_look]
do=_QXKeyTX
use=dwqx.dll
locke=pubring.txk
```

7. Сохраните публичную часть ключа Сервера доступа для передачи клиентам (публичная часть ключа используется для подключения клиентов к Серверу доступа).

8. Настройте файл quik.ini Сервера доступа.

- В секции [system] задайте наименование службы:

```
[system]
service=QuikDwellSubServer
service-desc=QUIK dwell sub server #1
```

- В секции [ctl_module] укажите порт для подключения Программы QMonitor к Серверу доступа, наименование ключа основного сервера и пароль этого ключа. Значения «name» и «password» можно скопировать из файла quik.ini основного сервера.

```
[ctl_module]
module=dwwqctl.dll
port=15121
name=broker
password=
```

- В секции [usend_module] укажите системное имя, порт для подключения пользователей к Серверу доступа, наименование ключа основного сервера и пароль этого ключа. Значения «name» и «password» можно скопировать из файла quik.ini основного сервера.

```
[usend_module]
module=dwsend.dll
sysname=Информационно-торговая система QUIK "broker"
name=broker
password=
port=15101
```



В поле «name» указывается наименование ключа основного сервера.

- В секции [dwell_module] укажите IP-адрес и порт для подключения Сервера доступа к основному серверу QUIK, наименование и пароль нового ключа для подключения пользователей. В параметре «auth_name» задайте наименование ключа основного сервера.

```
[dwell_module]
module=dtwcli.dll
address=192.168.1.1
port=15100
auth_name=broker
name=brokerSD
password=
```

- 9.** Установите службу Сервера доступа, используя команду:

```
quik.exe -install
```

- 10.** Настройте расписание ежедневного запуска и остановки Сервера доступа. Обычно расписание совпадает с расписанием основного сервера.
- 11.** Зарегистрируйте на основном сервере QUIK (с помощью программы QUIK Administrator) технологического пользователя Сервера доступа. Для этого пользователя в окне редактирования на вкладке «Общие права» установите флажок «Сервер доступа», а на вкладке «Права по классам» выберите шаблон прав «Менеджер» по всем необходимым классам.
- 12.** Запустите Сервер доступа и проверьте подключение Рабочим местом QUIK.

3.2 Установка Сервера доступа на ОС Linux

Пользователи для работы с сервисами под Linux

Для работы и управления сервисом применяются следующие пользователи:

- Администратор платформы:

Для обозначения этого пользователя используется имя root. Это пользователь, который знает пароль root либо добавлен в группу root, либо имеет доступ к широкому кругу команд на выполнение от имени root через утилиту sudo.



Пользователю доступна установка и удаление, а также администрирование сервиса: обновление, запуск и остановка.

- Пользователь, от имени которого работает сервис:

Для обозначения этого пользователя используется имя `arqasrv`. При установке сервиса по умолчанию создается пользователь именно с таким именем.

Пользователю также доступно администрирование сервиса: обновление, запуск и остановка – применяется, если выполнение администрирования пользователем `root` недоступно.

Таким образом, сервис всегда работает от имени пользователя `arqasrv`. Установка и удаление сервиса может производиться только пользователем `root`. Администрирование сервиса может производиться пользователями `root` или `arqasrv`.

Порядок установки

Установка сервиса производится пользователем `root`, вызовом `run`-файла.

По умолчанию все сервисы устанавливаются в директорию `/opt/arqasrv` и выполняются от имени системного пользователя `arqasrv`. Имя сервиса `<srvname>` для Сервера доступа по умолчанию совпадает с именем исполняемого файла – `quik`.

При установке наименование сервиса задается только строчными буквами.

Сервер доступа распространяется для установки на компьютеры с ОС Astra Linux в формате файла вида `<install_access_server-xx.xx.xx.run>`, где `xx.xx.xx` – версия продукта (далее `run`-файл). С помощью `run`-файла производится установка и обновление сервисов в системе.

Все указанные параметры можно переопределить соответствующими ключами запуска `run`-файла. Далее считаем, что выбраны параметры по умолчанию.

Начальные действия по установке сервиса (см. 1 – 5) должны производиться пользователем `root`. Для установки выполните следующие действия:

1. Скопируйте файл `install_access_server-xx.xx.xx.run` в директорию, на операции в которой у текущего пользователя есть права, например, домашний каталог (`/home/<user>` или `~/`).
2. Выполните команду добавления права на выполнение `run`-файлу:

```
chmod +x install_access_server-xx.xx.xx.run
```

3. Выполните команду установки сервиса:



```
sudo ./install_access_server-xx.xx.xx.run -i
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя. В процессе исполнения run-файла будут выполнены следующие действия:

- В случае отсутствия системного пользователя `arqasrv`, он создается с правами по умолчанию и включается в одноименную группу. В качестве домашней директории ему будет установлена директория `/opt/arqasrv`. От имени этого пользователя будет работать устанавливаемый сервис.
- В директории `/opt/arqasrv/quik` создается поддиректория с именем `quik`, в которую будут распакованы файлы дистрибутива устанавливаемого ПО.
- Пользователь `arqasrv` назначается владельцем всех файлов и поддиректорий в директории сервиса.
- В системе управления службами `systemd` регистрируется сервис с именем `quik` и запуском от имени системного пользователя `arqasrv`.
- В директории `/etc/arqasrv` создается файл с именем `quik` для фиксации параметров установки сервиса.
- В директории сервиса генерируются следующие командные файлы:
 - «`q_start.sh`» – запуск сервиса, в том числе с ключами запуска. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - «`q_stop.sh`» – остановка сервиса. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - «`q_status.sh`» – вывод информации о текущем состоянии сервиса. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - «`uninstall.sh`» – удаление сервиса. Предназначен для выполнения пользователем `root`;
 - «`postmigration.sh`» – выполнение дополнительных операций при миграции. Предназначен для выполнения пользователями `arqasrv` и `root`.

При успешной установке сервиса в консоль выводится сообщение:

«Installation of service “quik” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

Структура каталогов имеет значение. Перемещение или переименование файлов сервиса может привести к ошибке в установке.

4. Установите пакет `libjemalloc2` из официального репозитория Astra Linux. Для этого выполните в консоли команду:



```
sudo apt install libjemalloc2
```

Данная библиотека реализует механизмы работы с оперативной памятью, более подходящие для сценариев работы Сервера доступа, чем встроенные в систему по умолчанию.

5. Если управление установленным сервисом предполагается выполнять пользователем `arqasrv`, выполните следующие действия:

- Для предотвращения внесения пользователем `arqasrv` изменений в скрипты управления сервисом, на которые ему будет выдано разрешение выполнения от имени `root`, сделайте их неизменяемыми, выполнив следующие команды:

```
chattr +i /opt/arqasrv/quik/quik/q_start.sh  
chattr +i /opt/arqasrv/quik/quik/q_stop.sh
```

- Выдайте пользователю `arqasrv` права на выполнение скриптов управления сервисом от имени `root`, выполнив следующие действия:
 - Выполните команду:

```
sudo visudo
```

- В открывшемся `vi`-подобном редакторе добавьте строку:

```
arqasrv ALL=(root) /opt/arqasrv/quik/quik/q_start.sh,  
/opt/arqasrv/quik/quik/q_stop.sh
```

Эта строка разрешает пользователю `arqasrv` выполнять перечисленные скрипты на текущем компьютере от имени `root`.

Дальнейшие действия могут выполняться пользователем `arqasrv` или `root`.

6. Скопируйте секретную часть ключа основного сервера (обычно это файл `secrserv.txk` в папке основного сервера `QUIK`) в файл `secrserv.txk` в папке Сервера доступа (необходимо скопировать полностью файл или текст ключа текстовым редактором).
7. С помощью Программы для создания и управления ключами (`KeyGen`) сгенерируйте новый ключ для технологического пользователя Сервера доступа.
8. Зарегистрируйте технологического пользователя Сервера доступа в программе `QUIK Administrator`:



- Внесите пользователя в справочник «Пользователи»;
- На вкладке «Общие права» включите флажок «Сервер доступа»;
- Присвойте ему созданные ключи доступа.

Подробнее см. Руководство по администрированию QUIK Administrator п. 2.3.2.

- Из файла `secring.txk` с новым ключом добавьте в файл `secrserv.txk` секретную часть ключа технологического пользователя Сервера доступа. На Сервере доступа в `secrserv.txk` должно быть две секции: «от Сервера доступа» и «от основного сервера».
- Скопируйте `pubring.txk` нового ключа в папку Сервера доступа. Убедитесь, что в `pubring.txk` есть обе секции: «от Сервера доступа» и «от основного сервера».
- Проверьте, что в файле `qcrypto.cfg` Сервера доступа указаны следующие параметры:

```
SECRING=secrserv.txk
PUBRING=quik.dwq

[auth]
look=qcrypto.cfg,db_look
look=qcrypto.cfg,locke_look

[db_look]
do=_QXKey
use=libdwqx.so

[locke_look]
do=_QXKeyTX
use=libdwqx.so
locke=pubring.txk
```

- Сохраните публичную часть ключа Сервера доступа для передачи клиентам (публичная часть ключа используется для подключения клиентов к Серверу доступа).
- Настройте файл `quik.ini` Сервера доступа:

- В секции `[ctl_module]` укажите порт для подключения Программы QMonitor к Серверу доступа, наименование ключа основного сервера и пароль этого ключа. Значения «name» и «password» можно скопировать из файла `quik.ini` основного сервера.

```
[ctl_module]
module=libdwqctl.so
port=15121
```



```
name=broker
password=
```

- В секции [usend_module] укажите системное имя, порт для подключения пользователей к Серверу доступа, наименование ключа основного сервера и пароль этого ключа. Значения «name» и «password» можно скопировать из файла quik.ini основного сервера.

```
[usend_module]
module=libdwsend.so
sysname=Информационно-торговая система QUIK "broker"
name=broker
password=
port=15101
```

В поле «name» указывается наименование ключа основного сервера.

- В секции [dwell_module] укажите IP-адрес и порт для подключения Сервера доступа к основному серверу QUIK, наименование и пароль нового ключа для подключения пользователей. В параметре «auth_name» задайте наименование ключа основного сервера.

```
[dwell_module]
module=libdtwcli.so
address=192.168.1.1
port=15100
auth_name=broker
name=brokerSD
password=
```

14. Для сервиса, установленного по умолчанию, произведите первый запуск с ключом -clean из директории с установленным сервисом командой:

```
sudo ./q_start.sh -clean
```

либо из любой директории, отличной от директории сервиса командой:



```
sudo /opt/arqasrv/quik/quik/q_start.sh -clean
```

15. Настройте автоматику запуска и остановки сервиса. Для этого используйте в скриптах автоматики запуск командных файлов `q_start.sh` и `q_stop.sh`, расположенных в директории установленного сервиса.

Сервер доступа необходимо перезапускать ежедневно. Запуск должен производиться через небольшой промежуток времени после запуска основного сервера (3-5 минут). Остановку Сервера доступа необходимо производить на 3-5 минут раньше остановки основного сервера.

3.2.1 Ключи запуска установочного run-пакета под Linux

Run-файл поддерживает следующий набор ключей запуска:

-i [<srvname>]

Выполнение с этим ключом доступно только пользователю `root`.

Установка сервиса с именем `<srvname>`. Параметр `<srvname>` необязателен. При отсутствии используется имя сервиса по умолчанию, соответствующее имени исполняемого файла Сервера доступа – `quik`. При указании параметра пользователем, его значение приводится к нижнему регистру, и сервис устанавливается с именем в нижнем регистре.

Установка двух одноименных сервисов не допускается, даже в разные корневые директории. При попытке это сделать установка будет завершаться ошибкой.

-d <rootdir>

Ключ запуска, применяемый только при установке сервиса (в комбинации с `-i`) для указания корневой директории для установки сервиса, отличной от директории по умолчанию `/opt/arqasrv`. Это директория, в которой создается поддиректория **`<softwaredir>/<srvname>`**, в которую будут распакованы бинарные и конфигурационные файлы устанавливаемого ПО.

-n <srvusername>

Ключ запуска, применяемый только при установке сервиса (в комбинации с `-i`) для указания пользователя `<srvusername>`, который станет владельцем файлов сервиса и от имени которого будет работать устанавливаемый сервис. Имя пользователя по умолчанию: **`arqasrv`**.

-u [<srvname>]

Выполнение с этим ключом доступно пользователям `arqasrv` или `root`.

Обновление сервиса с именем `<srvname>`. Параметр `<srvname>` необязателен. При отсутствии используется имя сервиса по умолчанию, соответствующее имени исполняемого файла Сервера доступа – `quik`.



Расположение сервиса и имя пользователя-владельца сервера указывать не требуется, так как оно сохранено в `/etc/arqasrv/<srvname>`.

-e

Выполнение с этим ключом доступно любому пользователю.

Распаковка полного содержимого архива, включая конфигурационные ini-файлы. Распаковка производится в поддиректорию с именем, равным имени run-файла (без расширения `.run`), которая в случае отсутствия создается рядом с исполняемым файлом.

-h, -?

Выполнение с этим ключом доступно любому пользователю.

Вывод краткой информации об аргументах запуска.

Примеры:

Запуск run-файла для установки сервиса:

```
sudo ./install_access_server-xx.xx.xx.run -i quiksub -d /opt/customdir
```

Запуск run-файла для обновления сервиса:

```
sudo ./install_access_server-xx.xx.xx.run -u quiksub
```

Запуск run-файла для распаковки:

```
./install_access_server-xx.xx.xx.run -e
```

3.3 Миграция Сервера доступа с ОС Windows на ОС Linux

При миграции ПО с ОС Windows на ОС Astra Linux необходимо учитывать следующие ограничения Linux-версии по сравнению с Windows-версией:

1. Отсутствует поддержка криптопровайдера МР.
2. Для переноса ПО, работающего на ОС Windows, на компьютер с ОС Astra Linux:



- Версия ПО, которая переносится с ОС Windows, должна быть равна версии ПО, которая будет устанавливаться на ОС Astra Linux.
- Перенос должен осуществляться в строго неторговое время: после завершения торгов и остановки сервиса и до начала торгов, перед первым запуском сервиса.

Перенос сервиса выполняется в два этапа:

- Установка сервиса на ОС Astra Linux (производится пользователем root);
- Перенос конфигурации с ОС Windows (производится пользователем root или arqasrv).

Для переноса ПО с ОС Windows на ОС Astra Linux выполните следующий порядок действий:

1. Скопируйте файл `install_access_server-xx.xx.xx.run` в директорию, на операции в которой у текущего пользователя есть права, например, домашний каталог (`/home/<user>` или `~/`).
2. Выполните команду добавления права на выполнение run-файлу:

```
chmod +x install_access_server-xx.xx.xx.run
```

3. Выполните команду установки сервиса:

```
sudo ./install_access_server-xx.xx.xx.run -i
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя. В процессе исполнения run-файла выполняются следующие действия:

- В случае отсутствия системного пользователя `arqasrv`, он создается с правами по умолчанию и включен в одноименную группу. В качестве домашней директории ему будет установлена директория `/opt/arqasrv`. От имени этого пользователя будет работать устанавливаемый сервис.
- В директории `/opt/arqasrv/quick` создается поддиректория с именем `quick`, в которую будут распакованы файлы дистрибутива устанавливаемого ПО.
- Пользователь `arqasrv` назначается владельцем всех файлов и поддиректорий в директории сервиса.
- В системе управления службами `systemd` регистрируется сервис с именем `quick` и запуском от имени системного пользователя `arqasrv`.
- В директории `/etc/arqasrv` создается файл с именем `quick` для фиксации параметров установки сервиса.
- В директории сервиса генерируются следующие командные файлы:
 - `quick_start.sh` – запуск сервиса, в том числе с ключами запуска. Предназначен для выполнения пользователями `arqasrv` и `root`;



- «q_stop.sh» – остановка сервиса. Предназначен для выполнения пользователями arqasrv и root;
- «q_status.sh» – вывод информации о текущем состоянии сервиса. Предназначен для выполнения пользователями arqasrv и root;
- «uninstall.sh» – удаление сервиса. Предназначен для выполнения пользователем root;
- «postmigration.sh» – выполнение дополнительных операций при миграции. Предназначен для выполнения пользователями arqasrv и root.

При успешной установке сервиса в консоль выводится сообщение:

«Installation of service “quik” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

Структура каталогов имеет значение, перемещение или переименование может привести к сбою установки.

4. Установите пакет libjemalloc2 из официального репозитория Astra Linux. Для этого выполните в консоли команду:

```
sudo apt install libjemalloc2
```

Данная библиотека реализует механизмы работы с оперативной памятью, более подходящие для сценариев работы Сервера доступа, чем встроенные в систему по умолчанию.

5. Если управление установленным сервисом предполагается выполнять пользователем arqasrv, выполните следующие действия:

- Для предотвращения внесения пользователем arqasrv изменений в скрипты управления сервисом, на которые ему будет выдано разрешение выполнения от имени root, сделайте их неизменяемыми, выполнив следующие команды:

```
chattr +i /opt/arqasrv/quik/quik/q_start.sh
chattr +i /opt/arqasrv/quik/quik/q_stop.sh
```

- Выдайте пользователю arqasrv права на выполнение скриптов управления сервисом от имени root, выполнив следующие действия:



- _ Выполните команду:

```
sudo visudo
```

- _ В открывшемся vi-подобном редакторе добавьте строку:

```
argasrv ALL=(root) /opt/argasrv/quik/quik/q_start.sh,  
/opt/argasrv/quik/quik/q_stop.sh
```

Эта строка разрешает пользователю argasrv выполнять перечисленные скрипты на текущем компьютере от имени root.

6. Скопируйте из директории Windows-сервиса в директорию Linux-сервиса /opt/argasrv/quik/<srvname> следующие файлы (при их наличии):

- _ Основной файл настроек quik.ini;
- _ Общий файл настроек криптопровайдеров crypto.cfg;
- _ Другие файлы настроек *.ini с сохранением их расположения относительно директории установки сервиса;
- _ Файлы ключей (*.txk), каталоги сертификатов провайдеров:
 - _ Ключи secrserv.txk, pubring.txk – для настройки криптопровайдера crypto32;
 - _ Каталог certs – для настройки криптопровайдера OpenSSL_pr;
 - _ Каталог signalcom – для настройки криптопровайдера Signalcom_pr.

7. Приведите имена скопированных в предыдущем пункте файлов и директорий к нижнему регистру. Для этого выполните в директории /opt/argasrv/quik/<srvname> команду:

```
sudo ./postmigration.sh
```

8. Измените настройки в перенесенных файлах:

- _ Все упоминания динамических библиотек (*.dll) необходимо преобразовать в соответствующее наименование на Linux. Для этого к имени необходимо добавить префикс «lib», а расширение заменить на *.so, например:

```
module=dwdata.dll  
замените на  
module=libdwdata.so
```



- Список секций файла quik.ini, в которых указаны наименования динамических библиотек, которые необходимо преобразовать:

```
[data_module]
module=dwdata.dll
замените на
module=libdwdata.so

[dwell_module]
module=dtwcli.dll
замените на
module=libdtwcli.so

[conn_module]
module=dwxs.dll
замените на
module=libdwxs.so

[trans_module]
module=dwtrans.dll
замените на
module=libdwtrans.so

[auth_module]
module=dwqx.dll
замените на
module=libdwqx.so

[limits_module]
module=dwlimits.dll
замените на
module=libdwlimits.so

[usend_module]
module=dwsend.dll
замените на
module=libdwsend.so

[ctl_module]
module=dwwqctl.dll
замените на
module=libdwwqctl.so
```

```
[msg_module]
module=dwgtalk.dll
замените на
module=libdwgtalk.so

[archive_module]
module=dwarch.dll
замените на
module=libdwarch.so

[banner_module]
module=dwbanner.dll
замените на
module=libdwbanner.so
```

- Замените наименования динамических библиотек в файле qcrypto.cfg. Секции, в которых указаны наименования динамических библиотек:

```
[auth]
look=qcrypto.cfg,db_look
look=qcrypto.cfg,locke_look

[locke_look]
use=dwqx.dll
замените на
use=libdwqx.so

[db_look]
use=dwqx.dll
замените на
use=libdwqx.so
```

- В настройках криптопровайдеров файла qcrypto.cfg измените наименования динамических библиотек и регистр файла настроек, например:

```
[CryptoProviders]
openssl=1

[openssl]
Module=OpenSSL_Pr.dll
IniFile=OpenSSL_Pr.ini
замените на
[openssl]
```



```
Module=libopenssl_pr.so
IniFile=openssl_pr.ini
```

- Все упоминания путей к файлам и каталогам необходимо привести к виду, принятому в файловой системе Linux – обратные слэши («\») необходимо заменить на прямые («/»), например:

```
crypto_provider_ini_file=.\openssl_pr.ini
замените на
crypto_provider_ini_file=./openssl_pr.ini
```

- Перечень настроек quik.ini, которые содержат пути к файлам или директориям с примерами значений:

```
[ctl_module]
ip_address_file=ip.cfg
rest_users_file=restu.cfg

[usend_module]
suspect_data_file=stats/suspect.txt

[key_management]
key_info_file=key_info.ini

[dwell_module]
proxy_file_settings=quik.ini

[areas]
frontend=areas/frontend
msg_priv=areas/msg_priv
public=areas/public
company=areas/company
private=areas/private
unrestricted=areas/unrestricted
hasharchives=hasharchives
hasharchivesttp=hasharchivesttp

[archive_module]
minutes_dir=minutes
ttp_dir=ttp

[auth_module]
```



```
settings_file=grypto.cfg
```

- Перечень настроек grypto.cfg, которые содержат пути к файлам или директориям с примерами значений:

```
[auth]
mail_settings_file=grypto.cfg
arw_log=stats/arw.log

[locke_look]
locke=pubring.txk
```

- Отредактируйте путь к файлу баннера, если он настроен. Файлом конфигурации баннера считается первый найденный Сервером доступа *.ini-файл в директории /areas/banners. Например:

```
[url_set]
image=./banner.bmp
```

- Сетевые диски обычно монтируются к локальным каталогам, поэтому необходимо уточнить у сетевых администраторов точку монтирования и прописать путь к ней, например:

```
[areas]
Archives=\\minutes\qminreplicator\archive\
замените на
[areas]
Archives=/mnt/qminreplicator/archive
```

9. Настройте автоматику запуска и остановки сервиса. Для этого используйте в скриптах автоматики запуск командных файлов q_start.sh и q_stop.sh, расположенных в директории установленного сервиса.

Сервер доступа необходимо перезапускать ежедневно. Запуск должен производиться через небольшой промежуток времени после запуска основного сервера (3-5 минут). Остановку Сервера доступа необходимо производить на 3-5 минут раньше остановки основного сервера.



3.3.1 Настройка прокси для подключения пользователей

Сервер поддерживает протокол HAProxy версии 1 при обработке пользовательских подключений. При настройке прокси необходимо указать порт сервера, который прописан в секции [usend_module].

3.4 Удаление сервиса

Удаление на Windows

Для удаления сервиса выполните следующие действия:

1. Остановите службу Сервера Доступа. Сделать это можно через приложение «Службы», открытое от имени администратора, либо вкладку «Службы» диспетчера задач, также запущенного от имени администратора.
2. Выполните удаление службы Сервера Доступа путем выполнения команды в консоли, запущенной от имени администратора:

```
quik.exe -remove
```

3. Выполните удаление каталога Сервера Доступа.

Удаление на Linux

Удаление сервиса производится пользователем root вызовом скрипта uninstall.sh, который находится в каталоге соответствующего сервиса.

Далее приведен порядок действий при удалении сервиса с именем по умолчанию – quik.

Для удаления сервиса выполните следующие действия:

1. Остановите службу Сервера доступа из директории с установленным сервисом командой:

```
sudo ./q_stop.sh
```

либо из любой директории, отличной от директории сервиса, запуском команды:

```
sudo /opt/arqasrv/quik/quik/q_stop.sh
```



2. Если управление установленным сервисом выполнялось пользователем `arqasrv`, выполните следующие действия:

- _ Отмените у пользователя `arqasrv` права на выполнение скриптов управления сервисом от имени `root`, выполнив следующие действия:
- _ Выполните команду:

```
sudo visudo
```

- _ В открывшемся `vi`-подобном редакторе удалите строку:

```
arqasrv ALL=(root) /opt/arqasrv/quik/quik/q_start.sh,  
/opt/arqasrv/quik/quik/q_stop.sh
```

- _ Снимите признак неизменяемости со скриптов управления сервисом, выполнив следующие команды:

```
chattr -i /opt/arqasrv/quik/quik/q_start.sh  
chattr -i /opt/arqasrv/quik/quik/q_stop.sh
```

3. В директории установленного сервиса `/opt/arqasrv/quik/quik` запустите командный файл `uninstall.sh` командой:

```
sudo ./uninstall.sh
```

либо из любой директории, отличной от директории сервиса командой:

```
sudo /opt/arqasrv/quik/quik/uninstall.sh
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя. В результате выполнения команды выполняются следующие действия:



- Удаляется регистрация сервиса с именем quik в системе управления службами systemd.
- Удаляется файл /etc/arqasrv/quik, в котором были зафиксированы параметры установленного сервиса.
- Директория, в которой установлен сервис /opt/arqasrv/quik/quik, переименовывается в /opt/arqasrv/quik/quik.backup_YYYY.MM.DD_hh.mm.ss. Переименование, а не удаление директории производится на случай, если потребуются данные из нее. Если такой потребности нет, удалите эту директорию вручную.

При успешном удалении сервиса в консоль выводится сообщение:

«Removing of service “quik” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

4. Использование провайдера шифрования OpenSSL

4.1 Получение сертификата

Для получения шаблонов файлов настроек подключения через OpenSSL обратитесь в техническую поддержку QUIK.

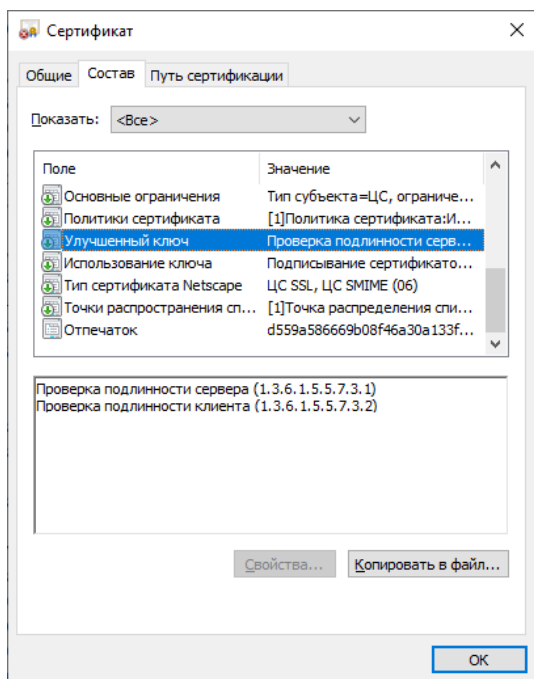
Перед выполнением настроек Сервера доступа для подключения к нему пользователей с помощью логина и пароля необходимо получить сертификат безопасности. Сертификат и ключ выдаются Службой Безопасности.

Процесс изготовления сертификата состоит из следующих этапов:

1. Генерация ключа.
2. Генерация запроса на сертификат.
3. Отправка запроса Удостоверяющему центру и получение сертификата.

В зависимости от выбранного Удостоверяющего центра процесс может меняться, но в свойствах получаемого сертификата всегда должно содержаться значение поля «Улучшенный ключ» – «Проверка подлинности сервера» (вкладка «Состав»):



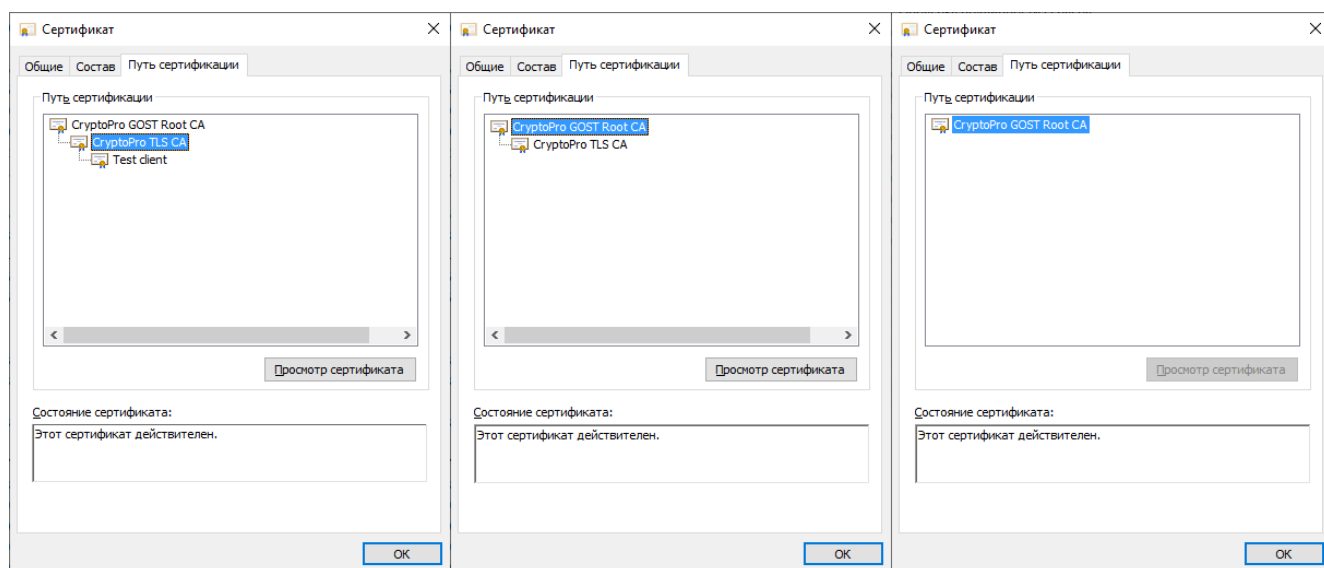


4.2 Подготовка сертификата

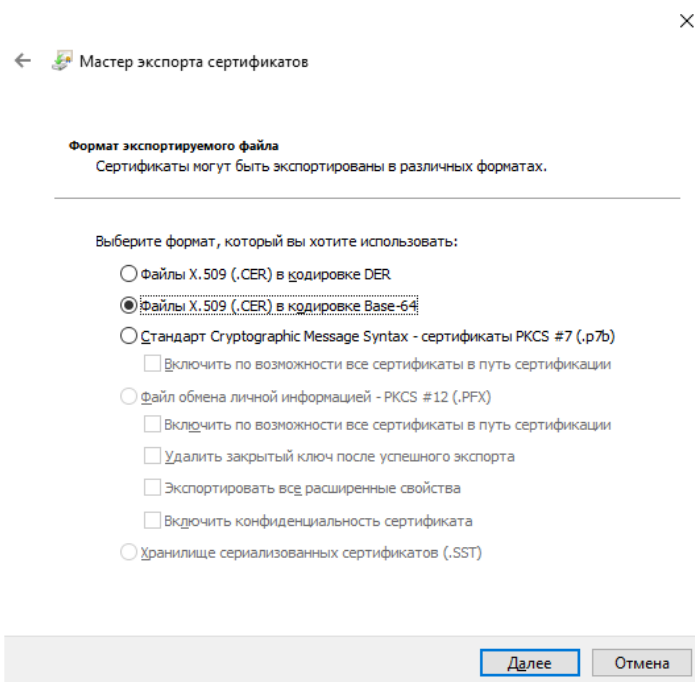
После получения сертификата и ключа, откройте и извлеките закрытый (*.key) и открытый (*.cer или *.crt) ключи. Если файлы имеют расширение *.pem, переименуйте: ключ в *.key, а сертификат в *.cer или *.crt.

1. Откройте для просмотра файл сертификата. В открывшемся диалоге сертификата перейдите на вкладку «Путь сертификации» и нажмите кнопку «Просмотр сертификата» на каждом сертификате (промежуточных сертификатов может быть два и/или более), чтобы отобразилась вся цепочка.

Самый последний сертификат в цепочке – корневой, для него кнопка «Просмотр сертификата» недоступна.



2. Перейдите на вкладку «Состав» и нажмите на кнопку «Копировать в файл...».
3. Сохраните каждый открытый ранее сертификат в отдельный файл, выбрав формат «Файлы X.509 (.CER) в кодировке Base-64»:



Рекомендуется использовать следующую схему наименования сертификатов, чтобы минимизировать ошибки:

- **root.cer** – корневой сертификат (корневой сертификат Удостоверяющего центра).
- **mid.cer** – сертификат промежуточного Удостоверяющего центра.
- **end.cer** – конечный сертификат (например, пользовательский).

4. Поместите файлы root.cer и mid.cer в отдельный каталог «Server\certs\CA».
5. Переместите файл end.cer в директорию «Server\certs\» и переименуйте в store.pem.

Сделайте копию готовой директории certs для дальнейшего применения при настройке Рабочего места QUIK или web2QUIK. Копию необходимо сделать перед выполнением следующего шага.

6. В текстовом редакторе откройте для чтения файл секретного ключа *.key и скопируйте в буфер его содержимое.
7. В текстовом редакторе откройте для чтения/записи файл store.pem, расположенный в директории «Server\certs\CA». Вставьте из буфера секцию секретного ключа



в следующем порядке: сверху секция сертификата, а секция секретного ключа под секцией сертификата.

1. Недопустимо изменение порядка расположения секций.
2. Недопустимо наличие дополнительных символов или пробелов до секции, между секциями и после секций.

Пример:

```
-----BEGIN CERTIFICATE-----
3kZMw8o0nMIIDhTCCAm2gAwIBAgIJANX6GM1211/yMA0GCSqGSIb3DQEBCwUAMEs
BAYTA1JVMQwwCgYDVQQIEwNOU08xDTALBgNVBAoTBVbYKMF0ATk8lZXiiJa0ir2K
ZXYxEDA0BgNVBeeqiQ0+P5A+SplAMTB2FycWEucnUwHhcNMjAwMjA1MDUxOTA0Wh
q8DyFaAfVBpSJK6JvvL2ZfPAFJ3dkrJTZitmczR4GGvjT0hSaccNMjEwMjA0MDUx
VUtaZ1fwY061E3NrnQDG31ib9tzrdPUhrP9uzwmZrEFSUUEXDTALBgNVBAsTBFFE
QevKUxQQCxlUajTTL/Gtaa2yOxDSv9c3m/wk2KslgQ0zYSjutJFqWC8=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA9FF9gmLCSLbiuRZ0WhUtCoTkt1w6vSfAruG09KVmjSOILAKC
QAt0q+Lz1i0Xa2QgT4D0ZonX9iuTgsxnuHaMkyllR2bDJRckse3e1gT3gRetylK
JmLt5m4HiCX00Lx37weC1oJwPcu5BJhLV/vaSQ0jyMtESGPWv44qcvutuxwaIRja
OZe10/y298rg1deWtFvNl3Pq3qgxBV2ApnsSVYc2Z7Mvg41TIOK0uaoxpMZzNVTZ
zwkgJb/IYgyN2rFGbIgdAoGAaZLIoeqfQK/DvSI4BhhV2o4wE2aQCetD9vKhpuWL
JyxCzAJBgNV42fwVXDRvGRfjt7EkKbZy1EMcNJYwmDI3JUavI7IYfM=
-----END RSA PRIVATE KEY-----
```

4.3 Настройка сервера QUIK

4.3.1 Настройка на Windows

1. Из архива, полученного после обращения в техническую поддержку QUIK, переместите файл Server\OpenSSL_Pr.ini в корневую директорию сервера QUIK. Редактировать файл не требуется.
2. В директории с сервером QUIK разместите каталог certs, в папку «certs\CA» поместите файлы root.cer и mid.cer, в папку «certs\» поместите файл end.cer и переименуйте его в store.pem.
3. Откройте для редактирования файл crypto.cfg и в секцию [CryptoProviders] добавьте строку:

```
openssl=1
```

4. Ниже добавьте секцию:



```
[openssl]
Module=OpenSSL_Pr.dll
IniFile=OpenSSL_pr.ini
```

Пример:

```
[CryptoProviders]
Placebo=1
openssl=1

[placebo]
Module=Placebo_Pr.dll
IniFile=

[openssl]
Module=OpenSSL_Pr.dll
IniFile=OpenSSL_pr.ini
```

- 5.** Откройте для редактирования файл quik.ini и в секцию [usend_module] добавьте строку:

```
crypto_provider_ini_fileOpenSSL=OpenSSL_pr.ini
```

Пример:

```
[usend_module]
module=dwsend.dll
name=quiktest
password=qwe
port=15100
crypto_provider_ini_fileOpenSSL=OpenSSL_Pr.ini
```

- 6.** Откройте для редактирования файл OpenSSL_Pr.ini, который должен находиться в папке с сервером QUIK и добавьте следующие настройки:

```
[General]
CertStoreFile=certs\store.pem
ServerCertificateKey=
```



7. В настройке ServerCertificateKey укажите пароль к ключу сервера. Пароль может быть зашифрован. Для шифрования в начале пароля указывается символ «\$». Если файл ключа сервера (в store.pem) не имеет пароля, то настройка может иметь любое значение, в том числе и пустое.
8. Добавьте в файл OpenSSL_Pr.ini следующую настройку:

```
[TLS Connection Settings]
ServerHandShakeScheme=12
```

Значение ServerHandShakeScheme=12 обеспечивает включение режима восстановления пароля и аутентификации по логину и паролю, если восстановление не нужно, то укажите значение ServerHandShakeScheme=4.

4.3.2 Настройка на Linux

1. Из архива, полученного после обращения в техническую поддержку QUIK, переместите файл server/openssl_pr.ini в корневую директорию сервера QUIK. Редактировать файл не требуется.
2. В директории с сервером QUIK разместите каталог certs, в папку «certs/ca» поместите файлы root.cer и mid.cer, в папку «certs/» поместите файл end.cer и переименуйте его в store.pem.
3. Откройте для редактирования файл crypto.cfg и в секцию [CryptoProviders] добавьте строку:

```
openssl=1
```

4. Ниже добавьте секцию:

```
[openssl]
Module=libopenssl_pr.so
IniFile=openssl_pr.ini
```

Пример:

```
[CryptoProviders]
Placebo=1
openssl=1
```



```
[placebo]
Module=libplacebo_pr.so
IniFile=

[openssl]
Module=libopenssl_pr.so
IniFile=openssl_pr.ini
```

- 5.** Откройте для редактирования файл quik.ini и в секцию [usend_module] добавьте строку:

```
crypto_provider_ini_file=openssl_pr.ini
```

Пример:

```
[usend_module]
module=libdwsend.so
name=quiktest
password=qwe
port=15100
crypto_provider_ini_file=openssl_pr.ini
```

- 6.** Откройте для редактирования файл openssl_pr.ini, который должен находиться в папке с сервером QUIK и добавьте следующие настройки:

```
[General]
CertStoreFile=certs/store.pem
ServerCertificateKey=
```

- 7.** В настройке ServerCertificateKey укажите пароль к ключу сервера. Пароль может быть зашифрован. Для шифрования в начале пароля указывается символ «\$». Если файл ключа сервера (в store.pem) не имеет пароля, то настройка может иметь любое значение, в том числе и пустое.
- 8.** Добавьте в файл openssl_pr.ini следующую настройку:

```
[TLS Connection Settings]
ServerHandShakeScheme=12
```



Значение ServerHandShakeScheme=12 обеспечивает включение режима восстановления пароля и аутентификации по логину и паролю, если восстановление не нужно, то укажите значение ServerHandShakeScheme=4.

4.4 Настройка сервера доступа

4.4.1 Настройка на Windows

1. Из архива, полученного после обращения в техническую поддержку QUIK, переместите файл Server\OpenSSL_Pr.ini в корневую директорию сервера QUIK. Редактировать файл не требуется.
2. В директории с Сервером доступа разместите каталог certs, в папку «certs\CA» поместите файлы root.cer и mid.cer, в папку «certs\» поместите файл end.cer и переименуйте его в store.pem.
3. Откройте для редактирования файл qcrypto.cfg и в секцию [CryptoProviders] добавьте строку:

```
openssl=1
```

4. Ниже добавьте секцию:

```
[openssl]  
Module=OpenSSL_Pr.dll  
IniFile=OpenSSL_pr.ini
```

Пример:

```
[CryptoProviders]  
Placebo=1  
openssl=1  
  
[placebo]  
Module=Placebo_Pr.dll  
IniFile=  
  
[openssl]  
Module=OpenSSL_Pr.dll
```



```
IniFile=OpenSSL_pr.ini
```

5. Откройте для редактирования файл quik.ini и в секцию [usend_module] добавьте строку:

```
crypto_provider_ini_file=OpenSSL_pr.ini
```

Пример:

```
[usend_module]
module=dwsend.dll
name=quiktest
password=qwe
port=15100
crypto_provider_ini_file=OpenSSL_Pr.ini
```

4.4.2 Настройка на Linux

1. Из архива, полученного после обращения в техническую поддержку QUIK, переместите файл Server/openssl_pr.ini в корневую директорию сервера QUIK. Редактировать файл не требуется.
2. В директории с Сервером доступа разместите каталог certs, в папку «certs/ca» поместите файлы root.cer и mid.cer, в папку «certs/» поместите файл end.cer и переименуйте его в store.pem.
3. Откройте для редактирования файл crypto.cfg и в секцию [CryptoProviders] добавьте строку:

```
openssl=1
```

4. Ниже добавьте секцию:

```
[openssl]
Module=libopenssl_pr.so
IniFile=openssl_pr.ini
```

Пример:



```
[CryptoProviders]
Placebo=1
openssl=1

[placebo]
Module=libplacebo_pr.so
IniFile=

[openssl]
Module=libopenssl_pr.so
IniFile=openssl_pr.ini
```

5. Откройте для редактирования файл quik.ini и в секцию [usend_module] добавьте строку:

```
crypto_provider_ini_file=openssl_pr.ini
```

Пример:

```
[usend_module]
module=libdwsend.so
name=quiktest
password=qwe
port=15100
crypto_provider_ini_file=openssl_pr.ini
```

4.5 Настройка Рабочего места QUIK для подключения по OpenSSL

В папке Рабочего места QUIK необходимо создать папку «certs», внутри папки «certs» папку «CA» и поместить в нее файлы сертификатов корневого (root.cer) и промежуточного Удостоверяющего центра (mid.cer), подробнее см в п. [4.2](#).

В папку Рабочего места QUIK скопируйте Front\OpenSSL_pr_client.ini из архива, полученного при обращении в техническую поддержку QUIK.

Переключите Рабочее место QUIK на OpenSSL, используя один из следующих способов:



1. Вручную:

- В файле qcrypto.ini добавьте / измените недостающие строки по примеру:

```
[CryptoProviders]
OpenSSL_Provider=1

[CryptoProvidersSettings]
CipherCryptoProvider=OpenSSL_Provider

[OpenSSL_Provider]
Module=.\OpenSSL_Pr.dll
IniFile=.\OpenSSL_pr_client.ini
```

- В файле OpenSSL_pr_client.ini секции [TLS Connection Settings] проверьте наличие настройки «CheckPeerCertificate»:

```
[TLS Connection Settings]
UsedHandShakeScheme=4
CheckPeerCertificate=1
```

2. Через Рабочее место QUIK:

- В окне «Настройки клиентского места» (**Система / Настройки / Основные настройки...**) выберите вкладку «Шифрование» (**Программа / Шифрование**) и нажмите на кнопку  «Шифровать с помощью СКЗИ».
- В открывшемся окне «Крипто-провайдеры» нажмите на кнопку «Добавить новый» и заполните параметры в окне «Добавление крипто-провайдера» следующим образом:
 - «Название» – OpenSSL_Provider;
 - «Описание» – OpenSSL_Provider;
 - «Файл исполняемого модуля» – D:\QUIK\Front\OpenSSL_Pr.dll;
 - «Файл настроек крипто-провайдера» – D:\QUIK\Front\OpenSSL_pr_client.ini.
- Нажмите на кнопку «Добавить».
- В окне «Крипто-провайдеры» выберите строку с OpenSSL в поле «Список установленных крипто-провайдеров» и нажмите на кнопку «Выбрать».
- В окне «Настройки клиентского места» на вкладке «Шифрование» нажмите на кнопку  «Настройки по умолчанию». В открывшемся окне в поле «Аутентификация» выберите «по имени и паролю» и нажмите «ОК».



4.6 Настройка подключения Web2QUIK по OpenSSL

Для настройки подключения Модуля web2QUIK к серверу, и HTTPS-подключения мобильных приложений к Модулю web2QUIK выполните следующие действия:

1. Из архива, полученного после обращения в техническую поддержку QUIK, переместите файл web2QUIK\OpenSSL_pr_client.ini в корневой директории web2QUIK. Редактировать файл не требуется.
2. В директории с web2QUIK разместите каталог certs.
3. В папку «certs\CA» поместите сертификаты нового Удостоверяющего центра (корневого и промежуточных – всю цепочку). Наименование сертификата должно быть равно значению в subject_hash, а расширение – «0», пример:

```
645912cb.0
```

Subject_hash можно получить самостоятельно, выполнив команду (на компьютере должен быть openssl.exe):

```
openssl.exe x509 -in org.crt -noout -subject_hash
```

Для получения информации о subject_hash, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

4. Откройте для редактирования файл web2quik.ini:

- В секции [General] добавьте строку:

```
openssl=1
```

- В секции [General] укажите путь и название до файла ключа и сертификата.

Пример:

```
[General]
openssl=1
cert_file=brokerru.crt
```



```
private_key_file=brokerru.key
```

1. Для подключения Модуля web2QUIK к серверу можно использовать одну пару ключ/сертификат, что и для подключения мобильных приложений к Модулю web2QUIK (HTTPS-подключение).
2. При необходимости использовать две разные пары ключ/сертификат вторая пара (подключение web2QUIK к серверу) может быть выпущена внутренней службой безопасности. Для этого подключения сертификаты могут быть «самоподписанными» (выпущенными не всемирно признанным Удостоверяющим центром).

5. Рекомендуется проконтролировать наличие настройки CheckPeerCertificate=1 в секции [General] файла web2quik.ini. Если настройка не задана, валидация сертификата сервера QUIK по сертификату Удостоверяющего центра не производится.

Пример:

```
[General]
...
CheckPeerCertificate=1
```

4.7 Добавление цепочки сертификатов УЦ в https-сертификат web2QUIK

Для некоторых версий ОС Android требуется наличие всей цепочки сертификатов. Порядок создания корректного сертификата для таких случаев, следующий:

1. Из файлов root.cer, mid.cer и end.cer, скопированных в п. [4.2](#), файл end.cer – конечный сертификат, выданный, например, для ресурса test.webquik.ru.
2. Откройте файл end.cer для редактирования в текстовом редакторе и после его секции добавьте секцию из файла mid.cer, а после нее – секцию root.cer.
3. Сохраните изменения и переместите файл в директорию web2QUIK. Переименуйте, если требуется.

Пример сертификата с цепочкой сертификатов Удостоверяющего центра:



```

-----BEGIN CERTIFICATE-----
pHAIV0oKHMfgosiLAlnMVG8Fo4TZfkQpcS0dWigtbCmHCYuGfjjm7cFhMasp8BD9
Jxq+wKvOw24diS8m51RBcONfXHMfgosiLA6PqBd+vaCpJh21Rn9Q51bw9z130oa1
KHBdzv1KCQyoEfupHd0J8h8GWLqI3dSvo8HMfgosiLAYKkeb0xKAfHG/arQvJ91w
2TpC/bBIVqY+LcLJh1feGGut4lpOSaP1NEUvJXwQIxSHMfgosiLAD/YGeXU0ljgg
PsR9le9RK92sVFfnZ/oetQIWs3EhwwCIvAaTNoZ6pPIaCVJc5hIwDHMfgosiLA9h2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEGzCCA/ugAwIBHMfgosiLAR2uhHbdBYLvFMNpzANBgkqhkiG9w0BAQwFADCB
16lFhd2zi+WJN44pDfwGF/Y4QHMFgosiLAvzxhFoYt/jmPQT2BVPi7Fp2RBgvGQq
6jG35LWjOhSbJuMLe/0CjraZwTiXWtb2qHHMFgosiLAk6s+go/lunrotEbaGmAhy
LcmsJWtyXnW0OMGuf1pGg+pRyrbxmRE1a6Vqe8YAsOfHMfgosiLA8azjUeqkk+B5
yOGBQMkKW+ESPMFgKuOXwIlCypTPRpgSabuY0MLTDXJLR27lk8QyHMfgosiLAj4K
00u/I5sUKUErmgQfky3xxz1HMfgosiLA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MAkHMfgosiLAR0IxGzAZBgNVBAGMEkdyZWFOZXIgdWVhY2hlc3RlcjEQA4GA1UE
BwwHU2FsZm9yHMfgosiLA1UECgwRQ29tb2RvIENBIExpbWl0ZWQxITAFBgNVBAMM
GEFBQSB0ZXJ0aWZpY2F0ZHMfgosiLANlczCCASIwDQYJKoZIhvcNAQEBBQADggEP
-----END CERTIFICATE-----

```

Порядок расположения сертификатов должен быть следующий:

- 1. Сертификат безопасности, выданный на доменное имя компании.**
- 2. Сертификат промежуточного Удостоверяющего центра.**
- 3. Сертификат корневого Удостоверяющего центра.**

4.8 Замена истекшего сертификата

Необходимо следить за сроком действия сертификата и выпускать новый сертификат не позднее чем за 2 недели до окончания срока действия текущего сертификата.

После получения нового сертификата и секретного ключа, необходимо повторно выполнить настройку сертификатов для Сервера доступа.

Если новый сертификат выпущен новым Удостоверяющим центром, необходимо принять меры по заблаговременному распространению новых сертификатов Удостоверяющего центра на терминалы пользователей.

Распространение сертификатов Удостоверяющего центра на терминалы QUIK предполагается вместе с пакетом обновления, расположенном на сервере QUIK или Сервере доступа, поэтому файлы рекомендуется разместить заранее в папке Areas\Frontend\x64\Release\certs\CA\ на сервере QUIK или Сервере доступа, чтобы терминалы успели принять новые сертификаты пока работает старый сертификат.

