



# **RADIUS protocol provider**

**Setup instruction**

**Version 2.0**



# Contents

|                                               |   |
|-----------------------------------------------|---|
| 1. Setup instruction.....                     | 3 |
| 1.1 qcrypto.cfg file format .....             | 3 |
| 1.1.1 [auth] section .....                    | 3 |
| 1.2 radius_pr.ini file format .....           | 4 |
| 1.2.1 [radius_general_settings] section ..... | 4 |

You may email your comments on this Instruction to: [quiksupport@argatech.com](mailto:quiksupport@argatech.com)



# 1. Setup instruction

To setup two-factor authentication on the basis of RADIUS protocol follow the next steps:

1. For the support of RADIUS authentication provider by the QUIK server, open the **crypto.cfg** file in the QUIK server directory and setup parameters in the [\[auth\]](#) section.
2. Create the RADIUS provider's **radius.pr.ini** configuration file in the QUIK server's directory, set the settings in the [\[radius general settings\]](#) section.
3. To setup two-factor authentication on the basis of RADIUS protocol for a QUIK user in the QUIK Administrator program, follow the steps:
  - In the **Users** dictionary (**QUIK server / Users** menu item, **Security** tab) enable the **Two-factor authentication** option and select the RADIUS authentication type;
  - In the **Logins for another authentication system** dictionary (**QUIK server / Security / Logins for another authentication system** menu item) specify user's name for RADIUS-server.

## 1.1 crypto.cfg file format

### 1.1.1 [auth] section

- **RADIUS\_Use** – enables RADIUS authentication usage. Valid values:
  - 0 (by default) – authentication is not used;
  - 1 – is used.
- **RADIUS\_Provider** – file path to the module's radius\_pr.dll library. Value by default: "" (empty). Recommended value: .\radius\_pr.dll. The required parameter. For Linux OS, the ./libradius\_pr.so value is used.
- **RADIUS\_Provider\_IniFile** – path to the module's configuration file. Value by default: "" (empty). Recommended value: .\radius\_pr.ini. For Linux OS, the ./radius\_pr.ini value is used.
- **RADIUS\_Wait\_tmo** – timeout of PIN code entry by user in seconds. The values of the parameter at the server and access server can be different. Value by default: 30.

For example:

```
[auth]
...
RADIUS_Use=1
RADIUS_Provider=.\radius_pr.dll
RADIUS_Provider_IniFile=.\radius_pr.ini
RADIUS_Wait_tmo=120
```



## 1.2 radius\_pr.ini file format

### 1.2.1 [radius\_general\_settings] section

- **shared\_secret** – key is used in the password encrypting algorithm. The keys of RADIUS-server and RADIUS-client must coincide. Therefore, several keys can be stored at the server – separate key for each client. Value by default: "" (empty). The required parameter.
- **connection\_ip** – ip v4 address of RADIUS-server. Value by default: "" (empty). The required parameter.
- **connection\_port** – port of RADIUS-server. Value by default: 1812.
- **time\_out** – timeout of receiving reply from server in milliseconds. If the reply is not received during the specified period, the request is repeated (if the quantity of attempts is not reached) or considered incorrect and deleted from the waiting queue. Value by default: 1000.
- **count\_attempt\_to\_sending\_message** – quantity of attempts to send a request to the server. Value by default: 3.
- **nas\_ip** – ip v4 address of QUIK-server. Value by default: "" (empty). The required parameter.
- **logFile** – path and file name with logs. Value by default: radius\_logfile.log.
- **logging** – logging parameter. Valid values:
  - \_ 1 – logging is enabled;
  - \_ 0 (by default) – logging is disabled.
- **logLevel** – logging level. Value by default: 3 – displays all information.

File example:

```
[radius_general_settings]
shared_secret=qwerty
connection_ip=192.168.37.202
nas_ip=192.168.37.202
logFile=./radius_logfile.log
logging=1
```

