



QUIK two-factor authentication

Administrator's manual

Version 8.8

The Quik logo, which consists of the word "quik" in a white, lowercase, sans-serif font, centered within a solid green circle.

quik

Contents

1. Description of QUIK two-factor authentication technology	2
2. Configuration of QUIK two-factor authentication	2
2.1 Settings in quik.ini	2
2.2 Settings in QUIK Administrator	7
3. Report on QUIK two-factor authentication	8
4. Procedure of password initial receiving / recovering	10
5. Procedure of logging in system by means of QUIK two-factor authentication method	12
Appendix. Actions for text templates	13

You may email your comments on this Manual to: quiksupport@arqatech.com



1. Description of QUIK two-factor authentication technology

Two-factor authentication of users at QUIK server was developed to increase the security of user operations. The functionality allows decreasing the possibility of unauthorized access because of losing or stealing access keys which can cause financial loss to user. At this keys can be stolen by viruses which can infect user's computer, if he does not comply with the information security policy (such rules as checking software for viruses on the regular basis, updating antivirus databases, deliberate internet using, timely updating Windows security system, etc.)

The main idea is that on logging into the system along with the standard parameters (name and password for secret key protection) a user enters some additional information – access password (hereinafter referred as PASSWORD) – that is not stored on his computer, and can be sent to a user via an alternative communication channel secured from a hacker. For this purpose the following communication channels were selected:

- Sending PASSWORD by means of SMS that is sent to the phone number that was preliminary specified by the user;
- Sending PASSWORD by means of e-mail that are sent to the address that was preliminary specified by the user;
- Receiving PASSWORD directly from the broker organization employee (hereinafter referred as BROKER) who serves the user (for example, by phone).

A new PASSWORD needs to be entered when a user tries to establish connection from the computer which was not used for connection establishing before (potentially key and password stealing can take place). To detect such a situation QUIK server identifies and saves parameters of each user connection on the basis of new two-factor authentication scheme and when connection parameter change is suspected it requests PASSWORD. The PASSWORD is sent to the user only by means of one selected connection channel.

2. Configuration of QUIK two-factor authentication

2.1 Settings in quik.ini

Open the **quik.ini** file from QUIK\Server\ directory with the QUIK server settings to edit. In section [quik_auth] set up the following parameters:

- FromAddress – sender address of the e-mails on two-factor authentication and password recovering.
- RetrievePassword – password recovering mode. Valid values:
 - _ 0 (by default) – disabled;
 - _ 1 – enabled.

If authentication by login and password is not used or two-factor authentication is disabled at server then the mode is disabled disregarding the parameter value.

- RetrievePasswordOnTerminalTypes – comma separated list of terminal types for which password recovery is allowed. Valid values:
 - _ ALL (by default) – all terminal types. If this code is selected, all other codes are ignored;
 - _ DESKTOP – QUIK Workstation;
 - _ IQUIKX – iQUIK X Workstation;
 - _ QUIKANDROIDX – QUIK Android X Workstation;
 - _ WEBQUIK – webQUIK Workstation.
- UseEmailOnRetrievePassword – send password by e-mail for recovery. Valid values:
 - _ 0 – option is disabled. Password is sent by SMS. Only when SMS is used as a second authorization factor;
 - _ 1 (by default) – enabled.
- NewRetrieveCodeTimeOut – comma separated list of time intervals before new confirmation code is requested. Intervals are specified in seconds. The 0 value means that new code can be requested immediately. Number of values in the list stands for the quantity of new confirmation code request attempts. For example, the value “0, 60, 120, 240” means that the user can request a new confirmation code four times exclusive of the code that is sent automatically. At this the first code can be requested immediately, the next one in a minute, and others in two and four minutes. Value by default: 0, 0, 0, 0, 0 (five new code requests without waiting).
- NewRetrieveCodeMaxAttempts – maximum quantity of attempts to enter the confirmation code. Value by default: 0 – attempts quantity is unlimited.
- RetrieveCodeProcessingTimeOut – maximum timeout in seconds of reply after the confirmation code is sent. Value by default: 0 (unlimited).
- TemporaryPasswordLength – length of the temporary password for authentication by login and password. Integer from 8 to 32. If a number that is not included in the interval is specified then the nearest interval bound is used. Value by default: 8.
- TemporaryPasswordSymbols – list of symbol sets that are allowed to be in a temporary password. Values in the list are separated by '|'. Valid values:

- _ Number – digits (0-9);
- _ Lowercase – lowercase letters (a-z);
- _ Uppercase – uppercase letters (A-Z);
- _ Underline – ‘_’;
- _ Minus – ‘-’;
- _ Space – ‘ ’.

At least one of the following values is required: Number, Lowercase, Uppercase. Value by default: Lowercase|Number.

- TemporaryPasswordMaxAttempts – maximum quantity of attempts to recover password per day. Value by default: 0 (unlimited).
- TemporaryPasswordValidityPeriod – temporary password validity period in minutes. Value by default: 0 (the password validity period is the same as the validity period of the permanent password). Maximum value: 1440.
- retry – number of attempts to enter PIN. Value by default: 0 (number of attempts is not restricted). Parameter filling is obligatory.
- Quik_Auth_Wait_TMO – time out while waiting for user to enter PIN in seconds. Value by default: 75.
- AddInfoOnRetrievePassword – type of additional data required for password recovery process start. Valid values:
 - _ 0 – is not requested;
 - _ 1 – email for two factor authentication;
 - _ 2 – phone number for two factor authentication;

Value by default:

- _ 1 (email), if [UseEMailOnRetrievePassword=1](#);
- _ 0 (is not requested), if [UseEMailOnRetrievePassword=0](#)).
- CheckLastDigitsInPhoneNumber – quantity of the last digits of phone number to be checked for coincidence. Is used if phone number is requested as additional information ([AddInfoOnRetrievePassword=2](#)). The zero value stands for full number checking for coincidence. Value by default: 10.
- PinCodeDefaultTransport – PIN delivery method. Valid values:
 - _ sms (by default);
 - _ email.

- **UnsuccessAuthMaxAttempts** – maximum quantity of authentication attempts in a trading session. The zero value means no restrictions for attempts quantity. Value by default: 10.
- **AlertOnUnsuccessAuth** – user notification of entering wrong authentication data the specified quantity of times. Valid values:
 - _ 0 – not notify;
 - _ 1 (by default) – notify.

The setting is used if the [UnsuccessAuthMaxAttempts](#) setting contains a value different from 0.

- **BlockTypeOnUnsuccessAuth** – type of blocking on entering wrong authentication data the specified quantity of times. Valid values:
 - _ 0 – not block;
 - _ 1 (by default) – block user for the time specified in settings;
 - _ 2 – reset user password.

The setting is used if the [UnsuccessAuthMaxAttempts](#) setting contains a value different from 0.

- **BlockPeriodOnUnsuccessAuth** – time in seconds of blocking user on entering wrong authentication data the specified quantity of times. Value by default: 10.

The setting is used if [BlockTypeOnUnsuccessAuth](#)=1.

- **Template<Language><Code of template type>FileName** – path to the file with the template of message on password recovery or with the code for two-factor authentication. For each template type a separate template file is to be created. Template texts can contain actions (for details see [Appendix](#)). In the setting name specify:

- _ <Language> – message language. Valid values:
 - _ Ru – Russian;
 - _ En – English;
 - _ Def – language is not defined. Can be used for templates of the 2ndFactorAuthSubject and 2ndFactorAuthText types.
- _ <Code of template type> – message type. Valid values:

Templates of the texts to be used for the password recovery procedure:

- _ **RetrievingNotSupported** – the text which is displayed if in the current configuration the QUIK server does not support the password recovery procedure for all users or for the current user;
- _ **MaxRetrievingAttempts** – the text which is displayed when a user tries to restore password, if the number of attempts is exceeded;

- UserUnknown – the text which is displayed if a user entered wrong login or e-mail for password recovery request;
- UnknownError – the text which is displayed if the Alert dispatch module is unavailable or if any other error of sending an SMS occurs;
- IncorrectCode – the text which is displayed if the user entered wrong code for password recovery confirmation;
- TooMuchErrorsForCode – the text which is displayed if the number of attempts to enter confirmation code is exceeded;
- TooMuchErrors – the text which is displayed if many errors occurred on new password request;
- RetrievingInfo – the text which is displayed in the **User identification** dialog box. This text is displayed in the dialog box for entering login and e-mail. The length is less than or equal to 700 symbols. The text can be unspecified (in this case the text is not displayed);
- InfoDescription – link to the password recovering rules. Is displayed in the **User identification** dialog box. The length is less than or equal to 100 symbols. The text can be unspecified (in this case the text is not displayed);
- InfoText – text of the password recovering rules. Is displayed on clicking the link in the **User identification** dialog box. The length is less than or equal to 4 kByte. Text format: standard (plain text). Is required if InfoDescription is specified;
- WaitForCode – text of the message which informs that the code for confirmation of the new password creation procedure was sent to the user. Is displayed in the **Password recovery confirmation** dialog box and in the notification which is displayed on clicking the **Send new password** button;
- PasswordSent – text of the message which informs that a new password was created and sent by e-mail;
- AddInfoTitle – additional field name;
- BlockOnUnsuccseccAuth – notification text that is displayed when user account is blocked as a result of entering wrong authentication data the specified quantity of times.

Templates of the texts (also in form of link to the file with the template text) to be sent to the users by SMS and e-mail:

- Code – text of the message with the confirmation code. Is sent with the one time confirmation code which is used to start the password recovery procedure. Is sent using the same method as method for sending the second factor for the QUIK two-factor authentication (usually by SMS). The length is less than or equal to 280 symbols (4 SMS);
- NewPasswordSubject – subject of the message with the temporary password. Is specified in the subject of the e-mail with the temporary password. The length is less than or equal to 128 symbols;
- NewPasswordText – text of the message with the temporary password. Is sent with the one time confirmation code which is used to start the password recovery

procedure. The e-mail is sent by the QUIK server. Text format: standard (plain) or HTML. The length is less than or equal to 4 kByte.

Templates for the message subjects and text with the two-factor authentication code:

- _ 2ndFactorAuthSubject – subject of the message with the second factor. Is sent when authentication by the second factor is passed. The length is less than or equal to 128 symbols;
- _ 2ndFactorAuthText – text of the message with the second factor. Is sent when authentication by the second factor is passed. The length is less than or equal to 4 kByte. Text format: standard (plain) or HTML. If a PIN for two-factor authentication is to be sent by SMS then the setting is ignored;
- _ PasswordChanged – notification of password change;
- _ PasswordChangedSubject – subject of the notification of password change;
- _ PasswordChangedText – text about password change;

To send an empty message, leave an empty string instead of the file name.

- Template<TemplateType>Type – template file format. The parameter is supported for the NewPasswordText and 2ndFactorAuthText template types. Valid values:
 - _ plain (by default) – standard text;
 - _ html – text in HTML.

2.2 Settings in QUIK Administrator

In QUIK Administrator do the following:

1. In user permissions set up dialog box on the Security tab tick the **Use two-factor authentication** option and select **QUIK** type of authentication.

☒ Use two-factor authentication

Choose application

Investor (Android)
Investor (iOS)
Quik AndroidX
Other

Other

☒ Set individual settings

Type of authentication: QUIK

Authentication for logging in

Additional parameters for two-factor authentication and password recovery

Set parameters: code word [Edit...]

Scratch cards: not specified [Edit...]

Do not ask the user for a verification code

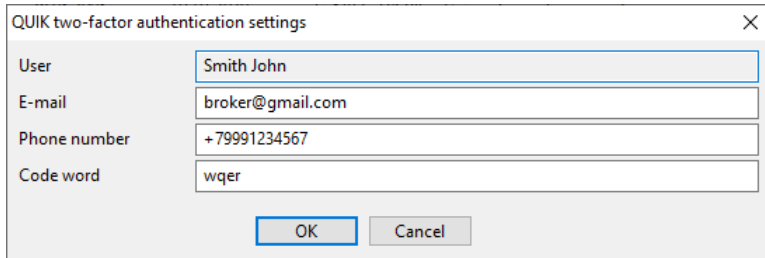
☒ days

- _ The **Do not ask the user for a verification code ... days** box stands for the number of days for which an additional password for QUIK two-factor authentication will not be

requested if the user doesn't change the connection parameters. Allowed values: integer numbers from 1 to 365.

- If changes of the connection parameters occur then an additional password will be requested. If the value 0 is specified then a new additional password will be requested every time a session is being established by the user. If the value is not specified then the additional password will be requested at the first connection to the server only.

2. On clicking **Edit...** the dialog box appears in which the following boxes for different ways of password delivery are available:



- **E-mail** – an email address to which an additional password will be sent.
- **Phone number** – a mobile number to which SMS will be sent. For this method of password delivery to work a broker should make integration with the Alert dispatch module.
- **Code word** – a code word which identifies a user when he contacts his broker to receive a password.

Methods of password delivery to a user can be used both separately and simultaneously.

3. Report on QUIK two-factor authentication

The report is intended to create a list of passwords for the users that establish connection by means of two-factor authentication. Only those users are displayed in the report which have **Code word** box filled in user permission settings.

The report is used, for example, if a client calls the broker and asks for the password for connection establishment. In this case the broker should create a report for the client and ask the client for the code word. The report can be created in QUIK Administrator (menu **QUIK server / Reports / Codewords...**).

Codewords

User

☐ by all users ☒ by one user

Smith John

OK Cancel

Only if the code word named by the client is correct a password for two-factor authentication can be told to the client.

Report on Quik two - factor authentication parameters

1 / 1

SAP CRYSTAL REPORTS

User ID 100101 Main Report

Date of report creation : 27.06.2019 11:29

Report on Quik two - factor authentication system

User ID:	100101
User name:	Smith John
Server password:	89101
Code word:	summer

Current Page No.: 1 Total Page No.: 1 Zoom Factor: 100%

The report can be created for all the clients who need password. To do this select **by all users**.

4. Procedure of password initial receiving / recovering

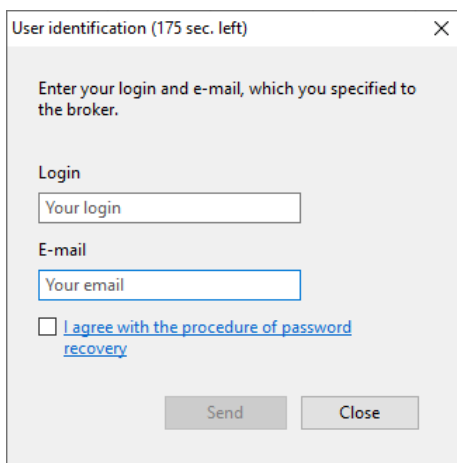
If a user does not know the password for authentication (the user has not yet received the password or has lost it), he can receive it without visiting broker and without participation of broker's employee.

Password recovery service operates if the following conditions are met simultaneously:

- Authentication by login and password is used for the user.
- Two-factor authentication of the QUIK type with second authentication factor sending by SMS is enabled.
- The user has phone number and e-mail for two-factor authentication specified in user's settings.
- The [RetrievePassword](#) setting in the [quik_auth] section of the quik.ini file is enabled.

When a user passes the procedure of password initial receiving / recovering the dialog boxes which are constructed by the broker by means of [templates](#) are displayed. The dialog boxes created on the bases of the templates supplied by default are shown below.

- In the **Login** dialog box a user clicks on the **Get password** button. The **User identification** dialog box is opened.



- The user enters login and e-mail and confirms that he reviewed the procedure of password recovery by ticking the checkbox.
- The server checks if two-factor authentication is enabled for the user and if authorization is not expired. If the check passed successfully the server sends an SMS with a confirmation code to the user.
- In the **Password recovery confirmation** dialog box the user enters the received code.

Password recovery confirmation (46 sec. left) X

You have been sent an SMS with a verification code.
Enter it in the textbox below to get a temporary password. After sending the old password will be invalid.

Pin code

[Send code again](#)

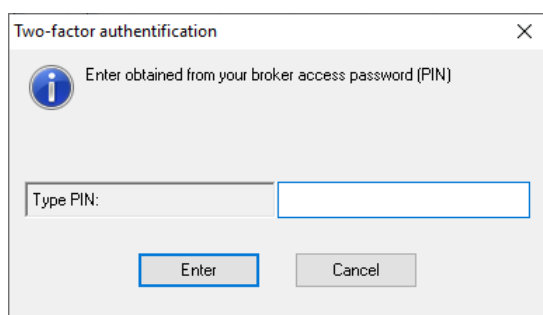
- The server checks the code, generates a temporary code and sends it to the user by e-mail.

5. Procedure of logging in system by means of QUIK two-factor authentication method

First part of the authentication procedure (by means of the access keys from the pubring.txk and secring.txk files or login and password) is standard – login and password are entered, and the server checks the entered parameters for correctness. If the first authentication part has passed successfully, then the QUIK server starts the second authentication part according to the following rules:

1. The QUIK server checks the parameters of the connection.
2. If the connection information is saved at server, the server checks if the connection is confirmed at the QUIK server (whether two-factor authentication passed on previous connection or not).
3. The connection expiration period is controlled (the expiration period is set up in QUIK Administrator in user settings, see sub-section [2.2](#)).

If all the checks passed successfully, then QUIK two-factor authentication is meant to be completed, and the user starts receiving data from the server. If at least one of the checks is not passed, then user must confirm new connection parameters by a new PASSWORD.



When a password entry dialog box is opened the password is sent to the client by the predefined connection channel – e-mail, SMS to the mobile phone or a call to the broker. If the last channel is used, the client must tell the code word to the broker. If the password that is entered in the box coincides with the required password, the new connection is meant to be confirmed.

If the password entry timeout has expired, the first authentication part (enter login and password for secret key security) is passed again.

Quantity of attempts to enter password is restricted. After the attempts quantity is exhausted user is temporarily blocked or password is reset. Information on user temporary blocking is available in QUIK Administrator in the user editing dialog box on the **Security** tab where blocking can also be removed.

Appendix. Actions for text templates

Texts of templates to be used for various notifications of password recovery can include actions.

All the actions have the following view: {CMD}, where CMD is command to insert some text parameter. A text can include free number of these commands, and one command can be included several times. To use symbol '{' or '}' type it in the text as '{{' or '}}' correspondingly.

Allowed actions:

- DATE – current date in format <DD.MM.YYYY>.
- TIME – current time in format <HH:MM:SS>.
- UID – identifier of the user (UID) whose password is recovered.
- USERNAME – user full name.
- PASSWORD – text of the temporary password.
- CODE – confirmation code. It is available only in a template of the Code type.
- EMAIL – e-mail for two-factor authentication.
- BLOCKEDTILL – date and time of user blocking expiration in format <DD.MM.YYYY HH:MM:SS>. Is used if [BlockTypeOnUnsuccessAuth](#)=1 and the value of [BlockPeriodOnUnsuccessAuth](#) differs from 0.