

RemoteView

Quick Guide: One Time Password



Index

- I. **Definition of OTP (One Time Password)**
- II. **Settings before using OTP**
- III. **2 ways to use OTP**
 - 1. **User mode**
 - 2. **Admin mode**
- IV. **Generating key as Admin**
- V. **Requesting key to Admin**

I. Definition of OTP (One Time Password)

■ OTP (One Time Password)

A one-time password (OTP) is a password generated using pseudo randomness or randomness that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication such as the vulnerability to replay attacks.



My Password is

II. Setting before using OTP

■ Pre-requisite to use OTP

In order to use 2-step verification (OTP), first users must contact us (see below) to enable the option.



E-mail: (support.us@rsupport.com) or



Call us: 1-888-348-6330

III. 2 ways to use OTP

■ Choosing the Mode (Admin or User)

- ① Log in (available for Admin only).
- ② Preferences
- ③ Company Settings
- ④ Select "Use 2-step verification (OTP)"
- ⑤ Choose the Mode

Use 2-factor verification (OTP) Use All Disabled

Set the 2-factor verification using One Time Password at the login.

OTP Configuration Admin mode User mode

Authentication Token can be configured by admin or by user.

Configure administrators Authentication Token from [My Profile](#).

Send Authentication Token

For user configuration, Authentication Token must be sent before applying to all.

■ Difference between Admin mode and User mode

| Feature | Admin | User |
|--------------------------------|--------------|--------------|
| View and manage all users' key | Yes | No |
| Register key | Admin | User |
| Reset key | All users | Own user |
| Mass distribute key | No | Yes |
| In case of lost key, | Admin issued | Indiv. email |

»Select the mode that best fits the business security policy and needs.

3.1. OTP | User Mode

■ Selecting User Mode

- ① Log in (available for Admin only)
- ② Preferences
- ③ Company Settings
- ④ Select "Use 2-step verification (OTP)"
- ⑤ Choose the User mode
- ⑥ Press Apply

The screenshot shows the RemoteView Preferences page. The 'Company Settings' tab is selected. Under 'More Security Settings', the 'Use 2-factor verification (OTP)' option is checked. The 'OTP Configuration' section shows 'Admin mode' and 'User mode' radio buttons, with 'User mode' selected and highlighted by a red box. Below this, there is a 'Send Authentication Token' button and a note: 'For user configuration, Authentication Token must be sent before applying to all.' An 'Apply' button is located at the bottom right of the page.

| RemoteView | Remote PC | LiveView | User Management | Organization | Statistics | Preferences |
|------------------------------|---|----------|-----------------|--------------|------------|-------------|
| PREFERENCES | 📱+📲 : for PC, Mobile 🖥️ : for PC only | | | | | |
| Company Information | Restrict access by MAC <input type="radio"/> Use All <input type="radio"/> Optional <input checked="" type="radio"/> Disabled | | | | | |
| Basic information management | More Security Settings 📱+📲 | | | | | |
| Company Settings | Session Expires After <input type="text" value="999"/> Min | | | | | |
| Unsubscribe | Set the available connection time <input type="radio"/> Use All <input type="radio"/> Optional <input checked="" type="radio"/> Disabled | | | | | |
| My Page | Password confirmation required in order to apply change. <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | |
| My Profile | Delete a standard user <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | |
| My Settings | Force to terminate a connection (Standard User) <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | |
| View Inquiries | This feature allows a user to disconnect an existing remote session to the PC and establish a new session. | | | | | |
| License Information | Security level of Password <input checked="" type="radio"/> Password strength : weak | | | | | |
| License Purchase Details | * Use 6~24 characters with uppercase, lowercase alphabets, numbers and symbols. | | | | | |
| Online Purchase History | <input type="radio"/> Password strength : normal | | | | | |
| Manage Coupon(s) | * Use 8~24 characters with uppercase, lowercase alphabets, numbers and symbols. | | | | | |
| Product Information | * 3 or more consecutive numbers cannot be used. | | | | | |
| RemoteView Information | <input type="radio"/> Password strength : strong (custom) | | | | | |
| Download | * Use 8~24 characters with uppercase, lowercase alphabets, numbers and symbols. | | | | | |
| | * 3 or more consecutive numbers cannot be used. | | | | | |
| | * Use uppercase, lowercase alphabets, numbers and symbols. | | | | | |
| | Set password expiration. <input checked="" type="checkbox"/> Set password expiration. <input type="text" value="30"/> days (Minimum of 1 to 90 days.) | | | | | |
| | Account will be locked after five unsuccessful attempts. <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | |
| | Use 2-factor verification (OTP) <input checked="" type="radio"/> Use All <input type="radio"/> Disabled | | | | | |
| | Set the 2-factor verification using One Time Password at the login. | | | | | |
| | OTP Configuration <input type="radio"/> Admin mode <input checked="" type="radio"/> User mode | | | | | |
| | Authentication Token can be configured by admin or by user. | | | | | |
| | Configure administrators Authentication Token from My Profile. | | | | | |
| | Send Authentication Token <input type="button" value="Send Authentication Token"/> | | | | | |
| | For user configuration, Authentication Token must be sent before applying to all. | | | | | |
| | <input type="button" value="Apply"/> | | | | | |

3.1 OTP | User Mode

■ Configuring User Mode – OTP

(After selecting User mode and pressing Apply)

- ① Press Generate Key



(Click on Generate Key to receive the Authentication Key to the registered email)

Verifying [Authentication Key]

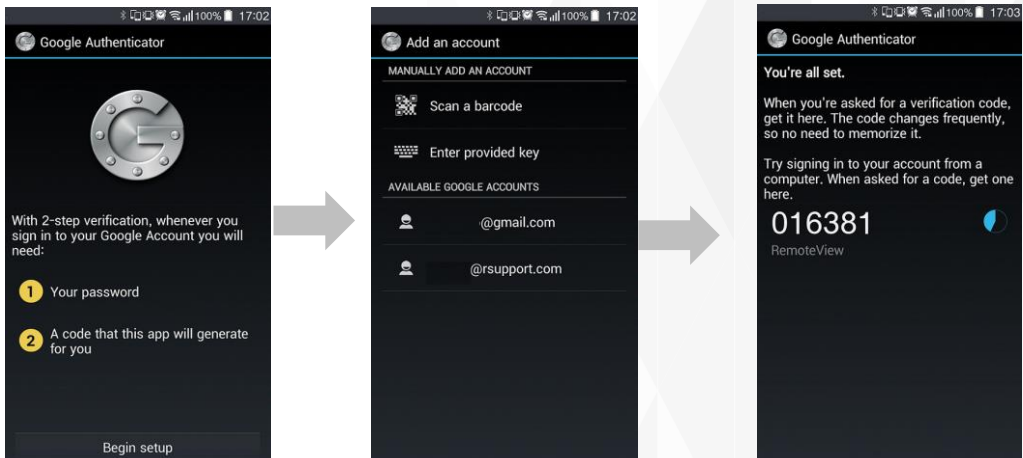
- ① Preferences
- ② My Profile
- ③ Google OTP key



- ② Registering Google OTP App (Adding Authentication Key)

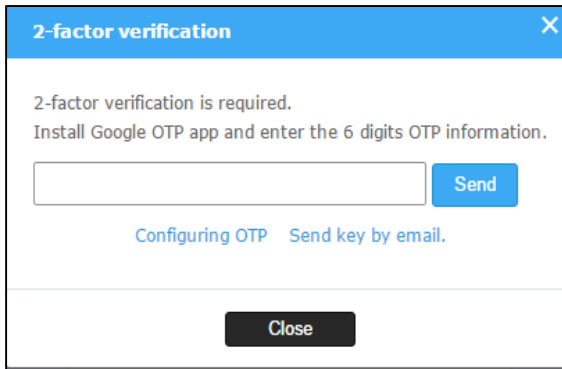
Adding [Authentication Key]

- >> Scan barcode or enter code.
- >> Install 'Google Authentication' from Google Play Store.



3.1 OTP | User Mode

(OTP Authentication will pop-up at the Web or Agent login.)

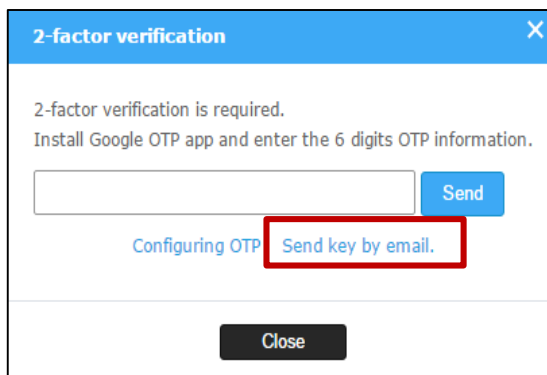


A screenshot of a "2-factor verification" pop-up window. The window has a blue header with the title "2-factor verification" and a close button (X). The main content area contains the text "2-factor verification is required. Install Google OTP app and enter the 6 digits OTP information." Below this text is a text input field and a blue "Send" button. At the bottom of the main content area, there are two links: "Configuring OTP" and "Send key by email." At the very bottom of the window is a dark grey "Close" button.

- ③ Launch Google Authentication App
- ④ Enter Google OTP 6 digit number

■ Configuring User Mode – Recovering key

In case the mobile device has been changed/lost, Authentication Key must be regenerated. To do this, click on "Send key via email" link to receive a new key.



A screenshot of the same "2-factor verification" pop-up window as above. In this version, the "Send key by email." link is highlighted with a red rectangular box. The rest of the window content is identical to the previous screenshot.

3.2. OTP | Admin Mode

■ Selecting Admin Mode

- ① Log in (available for Admin only)
- ② Preferences
- ③ Company Settings
- ④ Select "Use 2-step verification (OTP)"
- ⑤ Choose the Admin Mode
- ⑥ Press Apply

| RemoteView | | Remote PC | LiveView | User Management | Organization | Statistics | Preferences |
|------------------------------|--|-----------|----------|-----------------|--------------|------------|-------------|
| PREFERENCES | 🖥️+📱 : for PC, Mobile 🖥️ : for PC only | | | | | | |
| Company Information | Restrict access by MAC <input type="radio"/> Use All <input type="radio"/> Optional <input checked="" type="radio"/> Disabled | | | | | | |
| Basic information management | More Security Settings 🖥️+📱 | | | | | | |
| Company Settings | Session Expires After <input type="text" value="999"/> Min | | | | | | |
| Unsubscribe | Set the available connection time <input type="radio"/> Use All <input type="radio"/> Optional <input checked="" type="radio"/> Disabled | | | | | | |
| My Page | Password confirmation required in order to apply change. <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | | |
| My Profile | Delete a standard user <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | | |
| My Settings | Force to terminate a connection (Standard User) <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | | |
| View Inquiries | This feature allows a user to disconnect an existing remote session to the PC and establish a new session. | | | | | | |
| License Information | Security level of Password <input checked="" type="radio"/> Password strength : weak | | | | | | |
| License Purchase Details | * Use 6~24 characters with uppercase, lowercase alphabets, numbers and symbols. | | | | | | |
| Online Purchase History | <input type="radio"/> Password strength : normal | | | | | | |
| Manage Coupon(s) | * Use 8~24 characters with uppercase, lowercase alphabets, numbers and symbols. | | | | | | |
| Product Information | * 3 or more consecutive numbers cannot be used. | | | | | | |
| RemoteView Information | <input type="radio"/> Password strength : strong (custom) | | | | | | |
| Download | * Use 8~24 characters with uppercase, lowercase alphabets, numbers and symbols. | | | | | | |
| | * 3 or more consecutive numbers cannot be used. | | | | | | |
| | * Use uppercase, lowercase alphabets, numbers and symbols. | | | | | | |
| | Set password expiration. <input type="checkbox"/> Set password expiration. <input type="text" value="30"/> days (Minimum of 1 to 90 days.) | | | | | | |
| | Account will be locked after five unsuccessful attempts. <input type="radio"/> Use All <input checked="" type="radio"/> Disabled | | | | | | |
| | Use 2-factor verification (OTP) <input checked="" type="radio"/> Use All <input type="radio"/> Disabled | | | | | | |
| | Set the 2-factor verification using One Time Password at the login. | | | | | | |
| | OTP Configuration <input checked="" type="radio"/> Admin mode <input type="radio"/> User mode | | | | | | |
| | Authentication Token can be configured by admin or by user. | | | | | | |
| | Configure administrators Authentication Token from My Profile. | | | | | | |
| | <input type="button" value="Apply"/> | | | | | | |

3.2 OTP | Admin Mode

■ Configuring Admin Mode - OTP

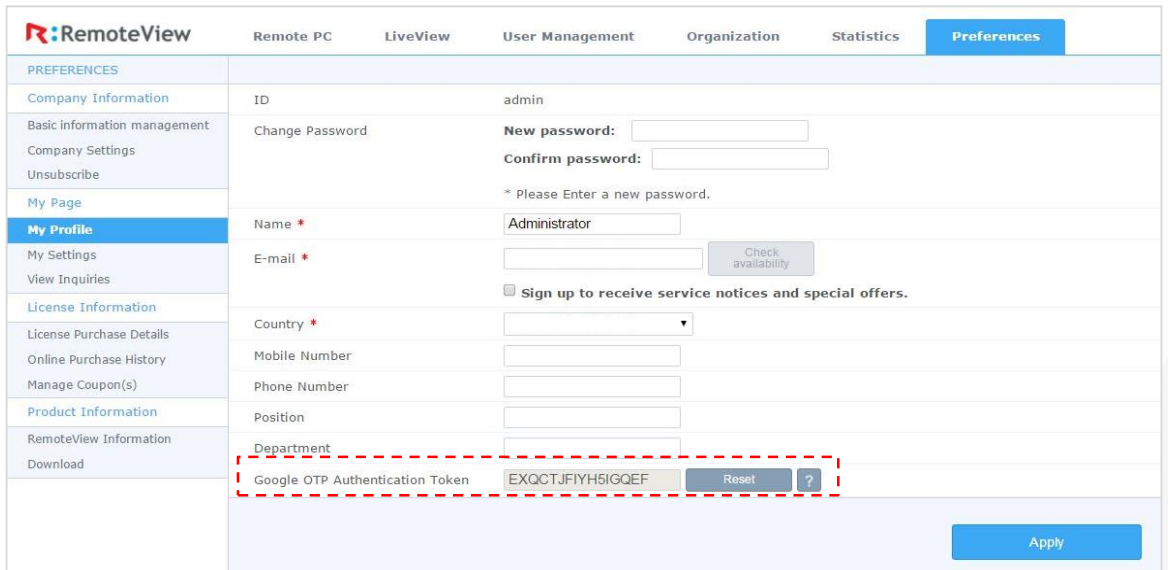
(After selecting Admin Mode and pressing Apply)

- ① Press Generate Key



Verifying [Authentication Key]

- ① Preferences
- ② My Profile
- ③ Google OTP key

A screenshot of the RemoteView web interface. The top navigation bar includes "RemoteView" and tabs for "Remote PC", "LiveView", "User Management", "Organization", "Statistics", and "Preferences". The "Preferences" tab is active. On the left is a sidebar menu with categories like "Company Information", "My Profile", "License Information", "Product Information", and "RemoteView Information". The main content area shows the "My Profile" section with fields for Name (Administrator), E-mail, Country, Mobile Number, Phone Number, Position, and Department. At the bottom of this section, the "Google OTP Authentication Token" is displayed as "EXQCTJFYH5IGQEF" with "Reset" and "?" buttons. A red dashed box highlights the token and its buttons. An "Apply" button is located at the bottom right of the form.

- ② Press Generate New Key



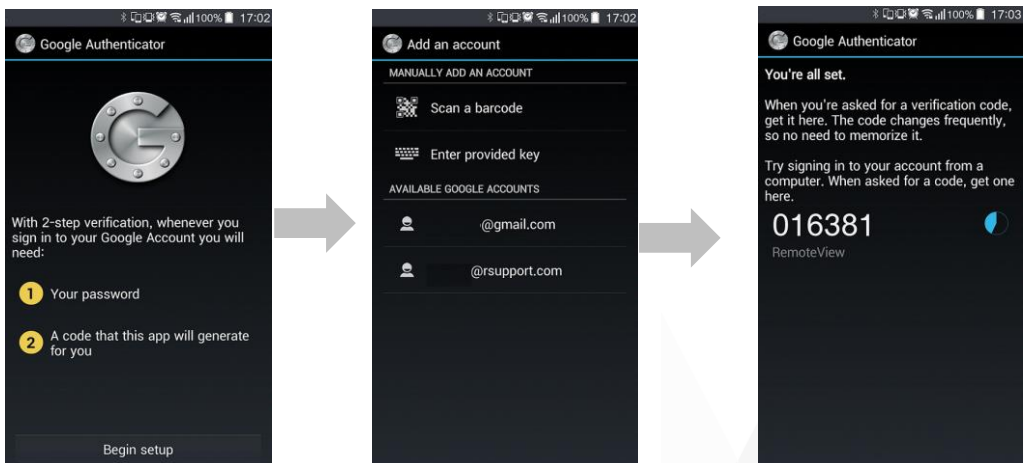
3.2 OTP | Admin Mode

③ Registering Google OTP App (Adding Authentication Key)

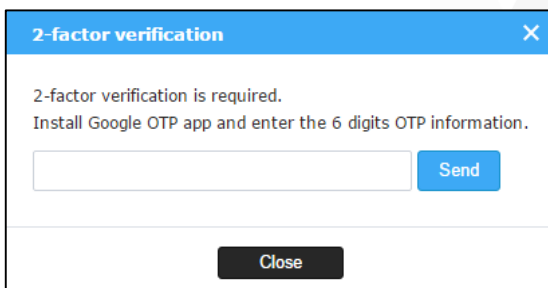
Adding [Authentication Key]

» Scan barcode or enter code.

» Install "Google Authentication" from Google Play Store.



(OTP Authentication will pop-up at the Web or Agent login)



④ Launch Google Authentication App

⑤ Enter Google OTP 6 digit number

3.2 OTP | Admin Mode

■ Configuring User Mode – Recovering Key

In case the mobile device has been changed/lost, Authentication Key must be regenerated.

Re-generate [Authentication Key]

- ① Preferences
- ② My profile
- ③ Google OTP Authentication Key

The screenshot displays the 'RemoteView' Admin interface. The top navigation bar includes 'Remote PC', 'LiveView', 'User Management', 'Organization', 'Statistics', and 'Preferences'. The left sidebar lists various settings categories, with 'My Profile' selected. The main content area shows the 'My Profile' settings, including fields for Name, E-mail, Country, and Mobile Number. A red dashed box highlights the 'Google OTP Authentication Token' field, which contains the value 'EXQCTJFIYH5IGQEF'. Below this field, there are 'Reset' and '?' buttons. An 'Apply' button is located at the bottom right of the form.

| RemoteView | | Remote PC | LiveView | User Management | Organization | Statistics | Preferences |
|------------------------------|---------------------------------|---|----------|-----------------|--------------|--------------------|-------------|
| PREFERENCES | | | | | | | |
| Company Information | ID | admin | | | | | |
| Basic information management | Change Password | New password: <input type="text"/> | | | | | |
| Company Settings | | Confirm password: <input type="text"/> | | | | | |
| Unsubscribe | | * Please Enter a new password. | | | | | |
| My Page | Name * | Administrator | | | | | |
| My Profile | E-mail * | <input type="text"/> | | | | Check availability | |
| My Settings | | <input type="checkbox"/> Sign up to receive service notices and special offers. | | | | | |
| View Inquiries | Country * | <input type="text"/> | | | | | |
| License Information | Mobile Number | <input type="text"/> | | | | | |
| License Purchase Details | Google OTP Authentication Token | EXQCTJFIYH5IGQEF | | | Reset | ? | |
| Online Purchase History | Department | <input type="text"/> | | | | | |
| Manage Coupon(s) | Google OTP Authentication Token | EXQCTJFIYH5IGQEF | | | Reset | ? | |
| Product Information | | | | | | | |
| RemoteView Information | | | | | | | |
| Download | | | | | | | |
| Apply | | | | | | | |


IV. OTP | Generating Key as Admin

■ Admin generating OTP Key for the user

- ① Log in as Admin
- ② Go to User Management
- ③ Select a user
- ④ Right-click on the mouse
- ⑤ Choose "Send OTP key via email"

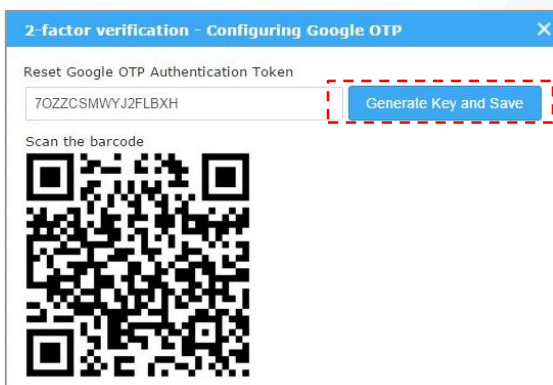


■ Admin re-generating OTP key for the user

- ① Log in as Admin
- ② Go to User Management
- ③ Change the view as List 
- ④ Select the user and press Reset



- ⑤ (Google OTP Authentication window pop-up)
Select Generate Authentication Key.



V. OTP | Requesting Key to Admin

■ User requesting a new OTP Authentication key to Admin

Users must request the Authentication Key to Admin in case of change/lost of mobile device to receive a new OTP Authentication Key.

Thanks

