Grandstream Networks, Inc.

GDMS MFA Device User Guide

Table of Content

OVERVIEW **4**

MFA DEVICE STANDARDS **5**

DOWNLOAD VIRTUAL MFA APPLICATION **6**

ENABLE MFA DEVICE **7**

Enable Virtual MFA Device 7

Enable Physical MFA Device 10

REMOVE MFA DEVICE **12**

GENERAL QUESTIONS **13**

Lost MFA Device/Invalid MFA Device 13

Table of Figures

Figure 1: Access Personal Information Page 7
Figure 2: Scan QR Code 8
Figure 3: Input MFA Secret Code 9
Figure 4: Hardware MFA Device Authentication 10
Figure 5: Physical MFA Device 11

Table of Tables

Table 1: MFA Device Standards 5
Table 2: Suitable Applications 6

OVERVIEW

GDMS Multi-Factor Authentication (MFA) is the simple and best security practice method that adds an extra protection to account username and password. When MFA is enabled, the user will be required to enter the login username and password (the first security method) and an authentication code (the second security method) from the MFA device when they log on to the GDMS platform. These multiple methods will improve the security for the settings and resources of your GDMS account.

Users can purchase supported physical devices or virtual MFA devices to enable MFA for GDMS accounts.

- **Virtual MFA Device**

Virtual MFA Device is an application that runs and simulates physical device on mobile phones or other devices. Virtual MFA device will generate a six-digit code based on a one-time time-synchronized cryptographic algorithm.

When logging into GDMS platform, the user must type in a valid code from the specific device. Each virtual MFA device assigned to the user must be unique. The user cannot type in the code with another user's virtual MFA device code for authentication. Since the virtual MFA device may be executed on unsafe mobile device, it may not provide the same level of security as physical MFA device.

- **Physical MFA Device**

Physical MFA Device is a device can generate a six-digit code based on a one-time time-synchronized cryptographic algorithm.

When logging into GDMS platform, the user must type in a valid code from the specific device. Each physical MFA device assigned to the user must be unique. The user cannot type in the code with another user's physical MFA device code for authentication.

MFA DEVICE STANDARDS

Table 1: MFA Device Standards

	Virtual MFA Device	Physical MFA Device
MFA Device	Refer to table 2	Purchase physical MFA device
Cost	Free	Price by supplier
Physical Device Standard	Use your smartphone/tablet/PC which can execute applications that support open TOTP standards to install virtual MFA device	The physical device which supports open TOTP standards. It is recommended to use the devices from Microcosm manufacturer.
Function	Support multiple tokens on single device	The financial service institutions and IT enterprises use the same model of device.

DOWNLOAD VIRTUAL MFA APPLICATION

Install virtual MFA application for your smartphone/tablet/PC from your device's app store. The following table lists some applications that are suitable for multiple kinds of smartphones.

Table 2: Suitable Applications

Android	Google Authenticator; Authy 2-Factor Authentication
iPhone	Google Authenticator; Authy
Windows Phone	Authenticator

ENABLE MFA DEVICE

To enhance security, it is recommended that users can configure Multi-Factor Authentication (MFA) to help protect GDMS resources. Users can enable MFA for GDMS accounts.

Enable Virtual MFA Device

Prerequisite: Users need to install virtual MFA application on the smartphone/tablet/PC before enabling virtual MFA device.

1. Log in to the GDMS platform with your account number, click on the name at the upper right corner, and access the personal information page:

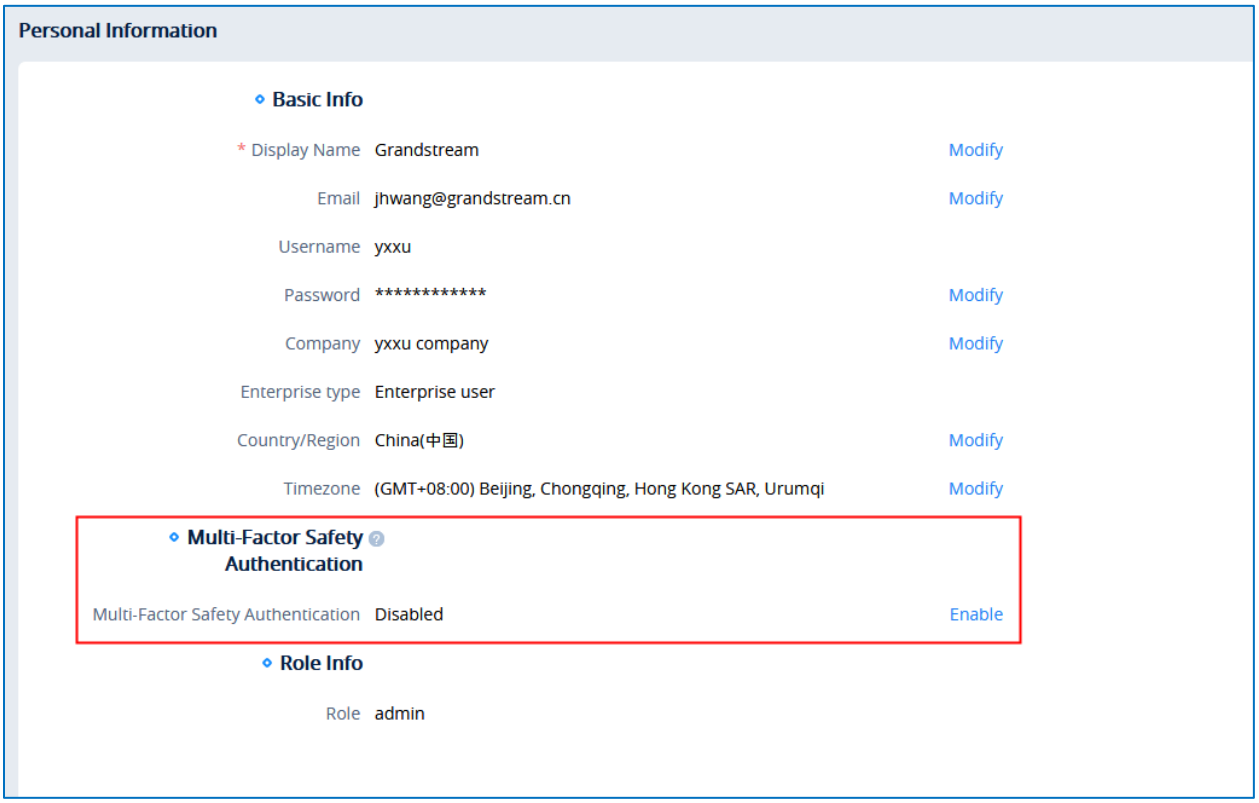

Figure 1: Access Personal Information Page

2. Click to enable "**Multi-Factor Safety Authentication**" option and select to use "**Virtual MFA Device**" on the pop-up window, then click "**Next**" option to continue.
3. Then, it will generate and display the configuration information of the virtual MFA device, including QR code graphics. This figure represents the configuration of the virtual MFA device as a secret key, users can scan the QR code to finish setting virtual MFA device. Users can also input the secret key manually

into the smartphone/tablet/PC in order to finish setting virtual MFA device if your smartphone/tablet/PC does not support to scan QR code.

Figure 2: Scan QR Code

4. Open virtual MFA application in your smartphone/tablet/PC, ensure that whether if the application in your smartphone/tablet/PC supports to scan QR code, and then perform one of the following actions below:
   a. If the MFA application in the smartphone/tablet/PC supports to scan QR code, the user can use the application to scan QR code to finish setting virtual MFA device. For example, the user can select the camera icon or scanning QR code option to use the device's camera to scan the QR code.
   b. If the smartphone/tablet/PC does not support to scan QR code, the user can click on "**show secret key"** option and input the private secret key manually in the MFA application.

Note: If a virtual MFA application supports multiple virtual MFA devices or accounts, the user can select the appropriate options to create new virtual MFA devices or accounts.

5. When the operations above are completed, users can use the virtual MFA device to generate one-time passwords.

   In the MFA secret code box Code 1, the user enters the one-time password which is displayed in the virtual MFA device currently. Then, wait for 30 seconds so that the virtual MFA device will generate a new one-time password, the user enters the second one-time password in the MFA secret code box Code 2.

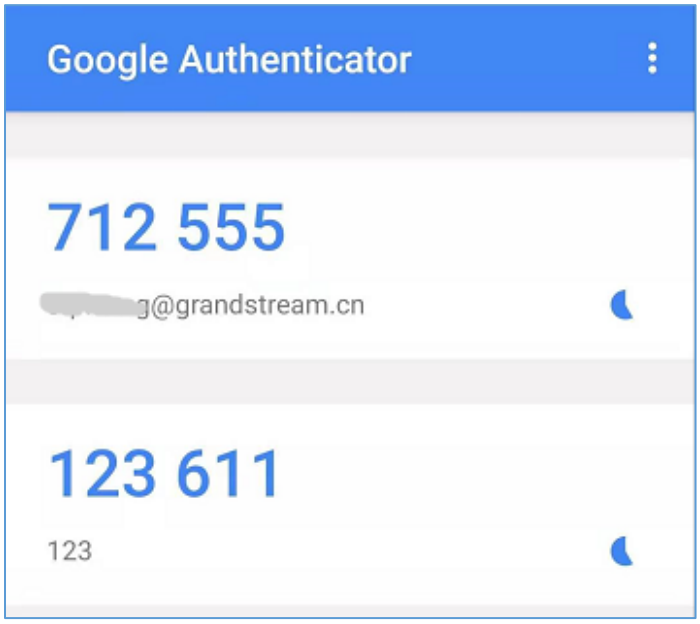

Figure 3: Input MFA Secret Code

6. Click on “Start Verification” option to start to verify the password. When the verification is pass, the GDMS account and the virtual MFA device has been bound successfully. When the user tries to log in the GDMS platform, the user must input the MFA device code.

Note:

1. When the secret code is generated, the user needs to use the secret code to proceed verification process immediately. If the user does not submit the secret code and wait for too long time, the one-time secret code (TOTP) may be expired. Then, the user may need to start the verification process again from the beginning.
2. The user can only bind the virtual MFA device to a single account.

Enable Physical MFA Device

Prerequisite: The user needs to purchase the physical MFA device before using this verification function.

1. Log in to the GDMS platform with your account number, click on the name at the upper right corner, and access the personal information page.
2. Click to enable "**Multi-Factor Safety Authentication**" option and select to use "**Physical MFA Device**" on the pop-up window, then click "**Next**" option to continue.
3. Enter the interface below to bind the physical MFA device with the GDMS account:

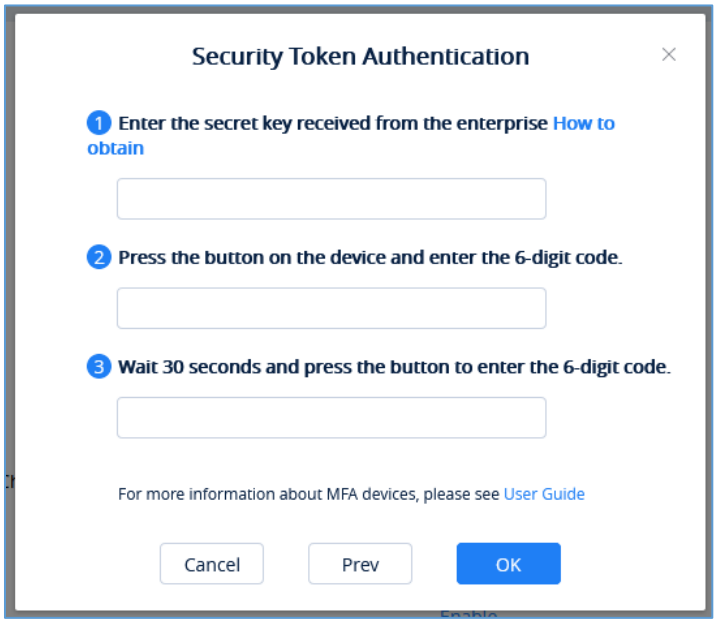

Figure 4: Hardware MFA Device Authentication

4. Input the secret key of the device. Please contact with the manufacturer for the secret key.

Note:

The key format is required to be "**DEFAULT HEX SEEDS**" (seeds.txt), or "**BASED32 SEEDS**".

Examples:

HEX SEED: B12345CCE6DA79B23456FE025E425D286A116826A63C84ACCFE21C8FE53FDB22

BASE32 SEED: WNKYUTRG3KE3FFTZ7UIO4QS5FBVBC2HJKY6IJLCP4QOH7ZJ12YUI====

5. In the MFA secret code box Code1, the user enters the six-digit one-time password which is displayed in the physical MFA device currently. The user needs to press the button on the front of the physical MFA device to display the secret code. Then, wait for 30 seconds and press the display button on the front of the physical MFA device again, so that the MFA device will generate the second six-digit one-

time password. The user needs to enter the second one-time password in the MFA secret code box Code 2.

Figure 5: Physical MFA Device

6. Click on “Start Verification” option to start to verify the password. When the verification is pass, the GDMS account and the physical MFA device has been bound successfully. When the user tries to log in the GDMS platform, the user must input the MFA device code.

Note:

1. When the secret code is generated, the user needs to use the secret code to proceed verification process immediately. If the user does not submit the secret code and wait for too long time, the one-time secret code (TOTP) may be expired. Then, the user may need to start the verification process again from the beginning.
2. The user can only bind the physical MFA device to a single account.

REMOVE MFA DEVICE

If the user does not need to proceed MFA verification, the user can remove the MFA device and restore normal login authentication method.

1. Log in to the GDMS platform with your account number, click on the name at the upper right corner, and access the personal information page.
2. Click "**Remove**" button to remove the MFA Authentication function for the current GDMS account.

GENERAL QUESTIONS

Lost MFA Device/Invalid MFA Device

If your MFA device is lost or does not work properly, you can remove the MFA device first and then re-enable the new MFA device.

Method 1: If your GDMS account is a sub-account, you can contact the main GDMS account to remove your multi-factor authentication from the **User** management page. After removal, you can log in to the GDMS platform with the password, and then re-enable the new MFA device.

Method 2: If your GDMS account is a main GDMS account and you cannot log in to the GDMS platform, you can contact our Technical Support, provide your relevant information to our Technical Support, and they will help you remove the multi-factor authentication (Our Technical Support will send the removal email to the user and the user needs to input account password and check removal).