

# Grandstream Networks Inc.

---

UCM6300 Series/UCM6300 Audio Series IP PBX

## **Multi-Factor Authentication User Guide**



## Table of Contents

<b>SUPPORTED DEVICES .....</b>	<b>4</b>
<b>INTRODUCTION .....</b>	<b>5</b>
Virtual MFA Device .....	5
Physical MFA Device .....	5
<b>MFA DEVICE SPECIFICATIONS .....</b>	<b>6</b>
<b>VIRTUAL MFA APPLICATIONS.....</b>	<b>7</b>
<b>USING MFA DEVICE .....</b>	<b>8</b>
Using Virtual MFA Device .....	8
Using Physical MFA Device .....	11
<b>REMOVING MFA DEVICE .....</b>	<b>13</b>
Removing MFA via User Management .....	13
Removing MFA via Login Page .....	13
<b>FAQ.....</b>	<b>14</b>
MFA Device Lost or Invalidated.....	14



## Table of Figures

Figure 1: Email Settings .....	9
Figure 2: User Information .....	9
Figure 3: Scan MFA QR Code .....	9
Figure 4: Enter MFA Code .....	10
Figure 5: Hardware MFA Device Certification .....	11
Figure 6: Physical MFA Device .....	12

## Table of Tables

Table 1: UCM Models Supporting Multi-Factor Authentication Feature .....	4
Table 2: MFA Device Specifications .....	6
Table 3: Virtual MFA Applications .....	7



## SUPPORTED DEVICES

Following table shows the UCM models supporting multi-factor authentication feature described in this guide:

**Table 1: UCM Models Supporting Multi-Factor Authentication Feature**

UCM Models Supporting Multi-Factor Availability Feature	
UCM6300 Series	
UCM6301	Firmware 1.0.10.5 or higher
UCM6302	Firmware 1.0.10.5 or higher
UCM6304	Firmware 1.0.10.5 or higher
UCM6308	Firmware 1.0.10.5 or higher
UCM6300 Audio Series	
UCM6300A	Firmware 1.0.10.5 or higher
UCM6302A	Firmware 1.0.10.5 or higher
UCM6304A	Firmware 1.0.10.5 or higher
UCM6308A	Firmware 1.0.10.5 or higher



## INTRODUCTION

The UCM Multi-Factor Authentication (MFA) feature adds a simple and secure method to protect the system on top of requiring username and password for login. If enabled, the UCM will require login credentials (the 1<sup>st</sup> factor) and a verification code from an MFA device (the 2<sup>nd</sup> factor), increasing security for the UCM system.

To use MFA, users will need to install a virtual MFA application or purchase a physical MFA device. MFA is configured and applied per account, not all accounts.

### Virtual MFA Device

Virtual MFA devices refer to software applications that are run on mobile devices or others to substitute physical MFA devices. An MFA application will generate a six-digit code via a time-based one-time password (TOTP) algorithm. This code will be required when logging into the UCM. The virtual MFA device assigned to each user must be unique. A user cannot use a code from another user's MFA device or application to log into his own account.

Since MFA applications may run on insecure hardware, they may not provide the same level of security as physical MFA devices.

### Physical MFA Device

A physical MFA device will generate a six-digit code via a time-based one-time password (TOTP) algorithm. This code will be required when logging into the UCM. The physical MFA device assigned to each user must be unique. A user cannot use a code from another user's MFA device or application to log into his own account.



## MFA DEVICE SPECIFICATIONS

**Table 2: MFA Device Specifications**

	<b>Virtual MFA Device</b>	<b>Physical MFA Device</b>
<b>Device</b>	See Table 3 below	Purchase required
<b>Cost</b>	Free	Price determined by 3 <sup>rd</sup> party vendor
<b>Device Specifications</b>	Any mobile device or tablet that can install and run applications supporting the TOTP standard	3 <sup>rd</sup> party vendor device that supports TOTP standard such as Microcosm MFA devices
<b>Application Scenario</b>	Multiple tokens can be supported on one device	Many financial institute and enterprise IT organizations use the same device type



## VIRTUAL MFA APPLICATIONS

Please go to your mobile device or tablet's app store to download and install MFA applications. The below table lists some example applications.

**Table 3: Virtual MFA Applications**

<b>Android Mobile Devices</b>	<a href="#">Google Authenticator</a> <a href="#">Twilio Authy 2-factor Authentication</a>
<b>iOS Mobile Devices</b>	<a href="#">Google Authenticator</a> <a href="#">Twilio Authy 2-factor Authentication</a>
<b>Windows Mobile Devices</b>	<a href="#">Authenticator</a> (by Microsoft)



## USING MFA DEVICE

It is highly recommended to configure Multi-Factor Authentication (MFA) to provide higher level security of the UCM system. Super admins and admins can toggle on MFA for their own accounts but not for others' accounts.

### Using Virtual MFA Device

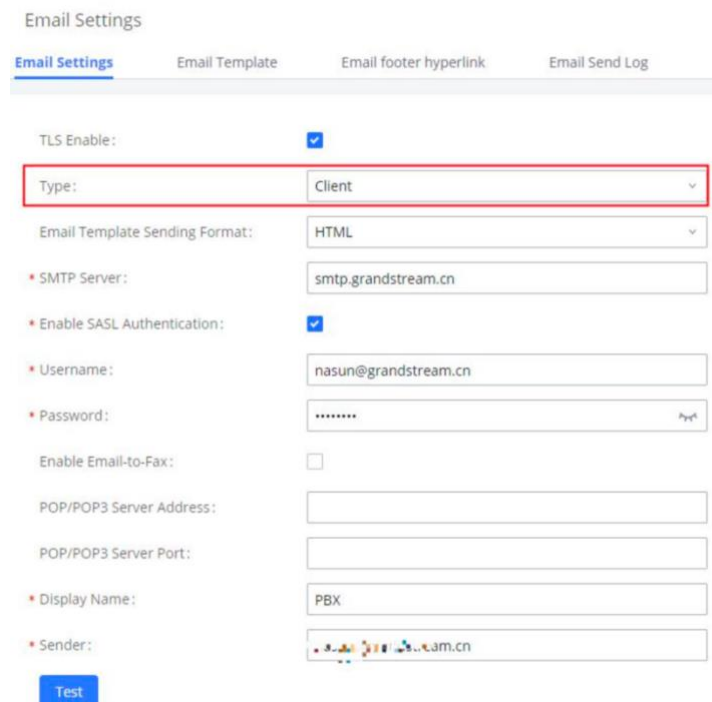
First, download an MFA application from your app store (e.g., Apple App Store or Google Play Store). See Table 3 for examples of available MFA applications.

**Note:**

To configure MFA properly, email addresses must be set for the UCM and the desired admin account. This is the only method to disable MFA without logging into the account. If no email address is configured, the account will not be able to log in.

Follow these steps to configure MFA on UCM:

1. Log into the UCM management portal with the super admin account. Navigate to System Settings→Email Settings and configure valid email settings that will allow UCM to send out emails. Make sure that the Type field is set to **Client**.



The screenshot shows the 'Email Settings' page with the following configuration:

- TLS Enable: ☒
- Type: Client (highlighted with a red box)
- Email Template Sending Format: HTML
- \* SMTP Server: smtp.grandstream.cn
- \* Enable SASL Authentication: ☒
- \* Username: nasun@grandstream.cn
- \* Password: [masked]
- Enable Email-to-Fax: ☐
- POP/POP3 Server Address: [empty]
- POP/POP3 Server Port: [empty]
- \* Display Name: PBX
- \* Sender: [empty]
- Test button





**Figure 1: Email Settings**

- On UCM web UI, navigate to Maintenance->User Management page, click to edit the user information. Configure email address for the admin.

Edit User Information: admin0 Cancel Save

Username:	<input type="text" value="admin0"/>	Privilege:	<input type="text" value="Super Administrator"/>
User Password:	<a href="#">Change Password</a>	Multi-Factor Authentication:	<input type="checkbox"/>
Email Address:	<input type="text" value="nasun@grandstream.cn"/>		


**Figure 2: User Information**

- Enable **Multi-Factor Authentication** and select **Virtual MFA device certification** in the prompt. Then click on next.
- The Virtual MFA device certification window will provide step-by-step instructions on setting everything up. Users can either scan a QR code or manually enter a key via their MFA app.

Virtual MFA device certification
×

① Install the app on your phone  
[Show application](#)

② Scan the QR code via the app on your virtual MFA device



You can also enter the key, [Show key](#)

③ Enter the MFA code on the app

\* Code1:

④ Wait for the code update, enter the second MFA code

\* Code2:

Cancel
Previous
Turn on authentication

**Figure 3: Scan MFA QR Code**

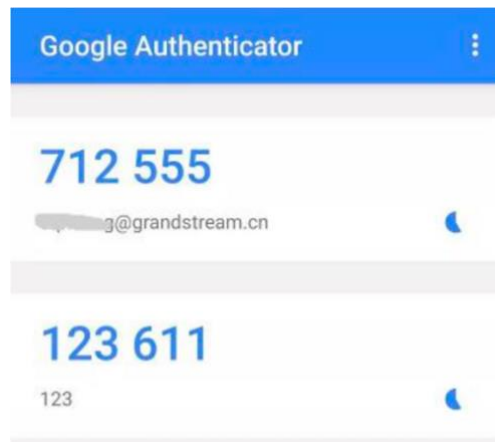


5. Open your virtual MFA app and follow the steps below.
  - (1) If your MFA application supports QR code, scan the provided QR code. Some mobile devices can scan and detect QR code using camera app.
  - (2) If your MFA application does not support QR code, click on “Show key” and then manually enter the key on the MFA application. If the MFA requires selecting how the code is generated, please select “Time-based”.

**Note:**

If virtual MFA application supports multiple MFA devices or accounts, please select adding new MFA device/account to create a new device or new account.

6. The MFA will periodically generate one-time passwords. Enter the displayed one-time password displayed on the MFA app into the Code 1 field. Wait approximately 30 seconds for the app to generate another one-time password. Enter this new password into the Code 2 field.



**Figure 4: Enter MFA Code**

7. Click on start authentication. After passing the authentication, click on **Save** and **Apply Changes** buttons for the settings to take effect. The account has now been successfully bound to the virtual MFA device. An MFA code will now be required to log into the account.

**Note:**

1. Please submit your request immediately after generating the code. Otherwise, the TOTP (time-based one-time password) will expire soon. If it's expired, please start over again.
2. One user can only be bound to one MFA device.



## Using Physical MFA Device

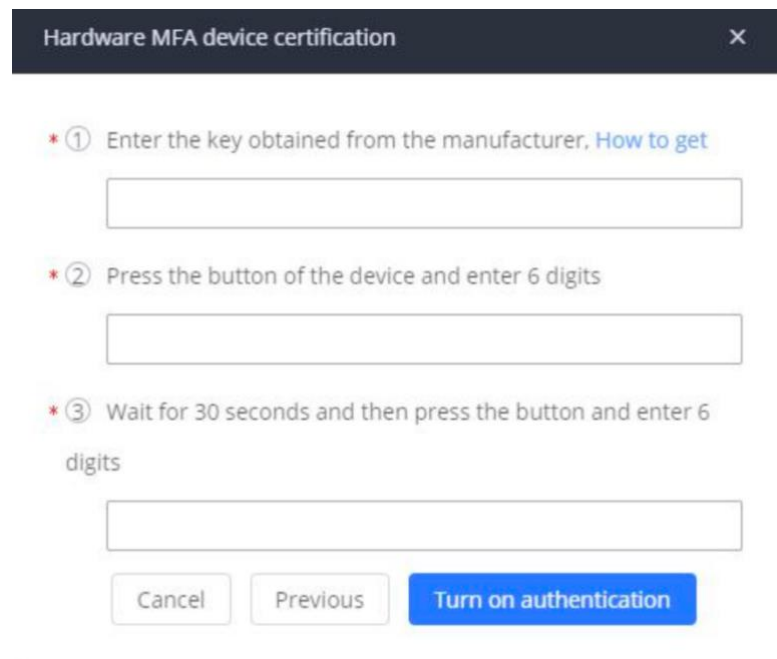
Users will need to purchase a physical MFA device and confirm that the UCM has valid email settings configured with the **Type** field set to **Client**. The account being set up for MFA must also have a valid email address configured.

### Note:

To configure MFA properly, email addresses must be set for the UCM and the desired admin account. This is the only method to disable MFA without logging into the account. If no email address is configured, the account will not be able to log in.

Here are the steps to configure MFA on UCM.

1. Log into the UCM management portal with the super admin account. Navigate to System Settings→Email Settings and configure valid email settings that will allow UCM to send out emails. Make sure that the Type field is set to **Client**.
2. On UCM web UI, navigate to Maintenance->User Management page, click to edit the user information. Configure email address for the admin.
3. Enable **Multi-Factor Authentication** and select **Virtual MFA device certification** in the following prompt. Then click on Next.
4. The following hardware MFA device certification window will appear:



Hardware MFA device certification

\* ① Enter the key obtained from the manufacturer, [How to get](#)

\* ② Press the button of the device and enter 6 digits

\* ③ Wait for 30 seconds and then press the button and enter 6 digits

Cancel Previous Turn on authentication

Figure 5: Hardware MFA Device Certification

5. Enter the device secret key. Please contact your vendor to obtain the secret key.



**Note:**

The secret key must be the default hex seeds (seeds.txt) or base32 seeds. For example,

HEX SEED: B12345CCE6DA79B23456FE025E425D286A116826A63C84ACCFE21C8FE53FDB22

BASE32 SEED: WNKYUTRG3KE3FFTZ7UIO4QS5FBVBC2HJKY6IJLCP4QOH7ZJ12YUI====

6. In **Code 1** field, enter the six-digit code displayed on the MFA device. You will need press the button on the front of the MFA device to display the code. Wait approximately 30 seconds for the device to generate a new code. Enter this second six-digit code into the **Code 2** field.



**Figure 6: Physical MFA Device**

7. Click on start authentication. After passing the authentication, click on save and apply for the settings to take effect. Now your account is successfully bind to the MFA device. MFA device code must be entered for the user to log in successfully.

**Note:**

1. Please submit your request immediately after generating the code. Otherwise, the one-time password may expire. If it's expired, please start over again.
2. Each user can only be bound to one MFA device.



## REMOVING MFA DEVICE

If MFA is no longer needed, MFA can be disabled for the account at any time.

### Removing MFA via User Management

1. Log into the admin account to disable MFA for. Navigate to **Maintenance→User Management** and edit the appropriate account.
2. Uncheck **Multi-Factor Authentication**.

### Removing MFA via Login Page

1. On the login page, enter the account credentials. Once the **Multi-Factor Authentication** window appears, click on the **Reset certification** link below the **Login** button.
2. An MFA removal email will be sent to the user's associated email address. In the email, click on the **Reset Now** button to confirm and disable MFA.
3. This reset email will be valid for 10 minutes and will expire immediately after a user clicks on it.



## FAQ

### MFA Device Lost or Invalidated

If your MFA device has been lost or no longer works, please follow the instructions below to unbind the MFA device and use a new MFA device.

1. On the login page, enter the account credentials. Once the **Multi-Factor Authentication** window appears, click on the **Reset certification** link below the **Login** button.
2. An MFA removal email will be sent to the user's associated email address. In the email, click on the **Reset Now** button to confirm and disable MFA.
3. This reset email will be valid for 10 minutes and will expire immediately after it is clicked on.

