



---

# GRANDSTREAM UCM63xx series IP-PBX Multi-Factor Authentication User Guide

May 28,  
2025

## Contents [ [hide](#) ]

- 1 UCM63xx series IP-PBX Multi-Factor Authentication
- 2 Product Information
  - 2.1 Multi-Factor Authentication Guide
  - 2.2 Specifications
  - 2.3 Virtual MFA Applications
- 3 Product Usage Instructions
  - 3.1 Using Virtual MFA Device
  - 3.2 Using Physical MFA Device
  - 3.3 Note:
- 4 Frequently Asked Questions (FAQ)
  - 4.1 Q: Can I use multiple virtual MFA devices with one IP-PBX account?
  - 4.2 Q: Is it mandatory to use MFA for all accounts in the IP-PBX system?
  - 4.3 Documents / Resources
    - 4.3.1 References

## UCM63xx series IP-PBX Multi-Factor Authentication

# Product Information

## Multi-Factor Authentication Guide

The IP-PBX Multi-Factor Authentication (MFA) feature adds an extra layer of security to the system by requiring a verification code in addition to the username and password for login.

## Specifications

| Device              | Cost                                 | Specifications   | Application Scenario   |
|---------------------|--------------------------------------|--|--|
| Virtual MFA Device  | Free                                 | Any mobile device or tablet supporting TOTP standard         | Enforce payment authentication methods and enhance e-commerce security |
| Physical MFA Device | Price determined by 3rd party vendor | 3rd party vendor device supporting TOTP or FIDO U2F standard | Used in financial institutions and enterprise IT organizations         |

## Virtual MFA Applications

To download MFA applications, visit your app store:

- Android™ Mobile Devices: Google Authenticator, Twilio Authy 2-factor Authentication
- iOS™ Mobile Devices: Google Authenticator, Twilio Authy 2-factor Authentication, Authenticator (by Microsoft)
- Windows™ Mobile Devices: Google Authenticator, Twilio Authy 2-factor Authentication

---

## Product Usage Instructions

# Using Virtual MFA Device

1. Download an MFA application from your app store (e.g., Apple App Store or Google Play Store).
2. Select a unique virtual MFA device application from the available options.
3. Follow the application's setup instructions to link it to your IP-PBX account.
4. Generate a six-digit code using the MFA application whenever logging into the IP-PBX.

# Using Physical MFA Device

1. Purchase a physical MFA device from a 3rd party vendor that supports TOTP or FIDO U2F standard.
2. Assign the physical MFA device to your IP-PBX account.
3. Use the generated six-digit code from the physical MFA device along with your login credentials when accessing the IP-PBX.

## Note:

MFA adds an extra layer of security to your IP-PBX system, ensuring only authorized users can access the system.

---

## Frequently Asked Questions (FAQ)

**Q: Can I use multiple virtual MFA devices with one IP-PBX account?**

A: Yes, multiple virtual MFA devices can be used with a single IP-PBX account for added security.

**Q: Is it mandatory to use MFA for all accounts in**

# the IP-PBX system?

A: No, MFA can be selectively enabled per account by super admins and admins, not mandatory for all accounts.

“

[View Fullscreen](#)



Multi-factor Authentication Guide

INTRODUCTION

The IP-PBX Multi-Factor Authentication (MFA) feature adds a simple and secure method to protect the system, in addition to requiring a username and password for login. If enabled, the IP-PBX will require login credentials (the 1st factor) and a verification code from an MFA device (the 2nd factor), increasing security for the IP-PBX 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.

Note: The term IP-PBX in this guide refers to the UCM63xx series, CloudUCM, SoftwareUCM, and GCC6000 Series (PBX module).

### Virtual MFA Device

Virtual MFA devices refer to software applications that are run on mobile devices or other devices 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 IPPBX. 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 their 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 IP-PBX. 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 their account.

## MFA DEVICE SPECIFICATIONS

Device Cost Device Specifications Application Scenario

### Virtual MFA Device

### Physical MFA Device

See Virtual MFA Applications table below

TOTP Hardware Token

FIDO Security Key

Free

Price determined by 3rd party vendor

Price determined by 3rd party vendor

Any mobile device or tablet that can install and run applications supporting the TOTP standard

3rd party vendor device that supports TOTP

Standard devices such as Microcosm MFA devices

Devices that support FIDO U2F open authentication standard.

Multiple tokens can be supported on one device

Many financial institute and enterprise IT organizations use the same device type

Enforce payment authentication methods and strengthen the security of e-commerce transactions.

## VIRTUAL MFA APPLICATIONS

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

Android™ Mobile Devices iOS™ Mobile Devices Windows™ Mobile Devices

Google Authenticator Twilio Authy 2-factor Authentication

Google Authenticator Twilio Authy 2-factor Authentication

Authenticator (by Microsoft)

## USING MFA DEVICE

It is highly recommended to configure Multi-Factor Authentication (MFA) to provide a higher level of security for the IP-PBX system. Super admins and admins can toggle on MFA for their 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 IP-PBX 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 the IP-PBX: 1. Log in to the IP-PBX management portal with the super admin account. Navigate to System Settings Email Settings and configure valid email settings that will allow IP-PBX to send out emails. Make sure that the Type field is set to Client.

Email Settings 2. On the IP-PBX web UI, navigate to the Maintenance User Management page, and click to edit the user information. Configure the email address for the admin.

User Information 3. Enable Multi-Factor Authentication and select the Authentication App in the prompt. Then click on next.

4. 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.

Authentication App Instructions 5. Open your virtual MFA app and follow the steps below.

If your MFA application supports a QR code, scan the provided QR code. Some mobile devices can scan and detect QR codes using a camera app. If your MFA application does not support QR codes, 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 the virtual MFA application supports multiple MFA devices or accounts, please select Add 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.

Enter MFA Code 7. Click on start authentication. After passing the authentication, click on the 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. Notes

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 IP-PBX 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 IP-PBX 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.

#### Configure TOTP Hardware Token

Below are the steps to configure a time-based one-time password (TOTP) hardware token on IP-PBX. 1. Log in to the IP-PBX management portal with the super admin account. Navigate to System Settings>Email Settings and configure valid email settings that will allow IP-PBX to send out emails. Make sure that the Type field is set to Client. 2. On the IP-PBX web UI, navigate to the Maintenance>User Management page, and click to edit the user information. Configure the email address for the admin. 3. Enable Multi-Factor Authentication and select TOTP Hardware Token in the following prompt. Then click on Next. 4. The following hardware MFA device certification window will appear: TOTP Hardware Token Certification Instructions 5. Enter the device's 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 the



Code 1 field, enter the six-digit code displayed on the MFA device. You will need to 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.

#### 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 bound to the MFA device. MFA device code must be entered for the user to log in successfully. Notes

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.

#### Configure FIDO Security Key (CloudUCM Only)

Please follow the steps below to configure FIDO security key authentication for CloudUCM: 1. Log in to the CloudUCM management portal with the super admin account. Navigate to System SettingsEmail Settings and configure valid email settings that will allow CloudUCM to send out emails. Make sure that the Type field is set to Client. 2. On the CloudUCM web UI, navigate to the MaintenanceUser Management page, and click to edit the user information. Configure the email address for the admin. 3. Enable Multi-Factor Authentication and select FIDO Security Key in the following prompt. Then click on Next. 4. Select where to store your passkey: on your iPhone, iPad, Android device, or a physical security key.

Storage Method for FIDO Passkey 5. If an iPhone, iPad, or Android device is selected, a QR code will be displayed on the next screen to be scanned using the device's camera.

If a

security key is chosen, the key will need to be inserted into the computer's USB port.

#### Saving Passkey on iPhone, iPad, or Android Device

Saving Passkey on a Security Key 6. Follow the instructions based on the selected method. Once completed, a confirmation window will appear to verify that FIDO authentication

has been successfully enabled.

FIDO Authentication Enabled Successfully

## 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 in to the admin account to disable MFA. 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.

## SUPPORTED DEVICES

The following table shows all the IP-PBX models that support the multi-factor authentication feature:

Model UCM6301 UCM6302 UCM6304 UCM6308 UCM6300A UCM6302A UCM6304A

Minimum Firmware Version Firmware 1.0.11.10 or higher Firmware 1.0.11.10 or higher  
Firmware 1.0.11.10 or higher Firmware 1.0.11.10 or higher Firmware 1.0.11.10 or higher

Firmware 1.0.11.10 or higher Firmware 1.0.11.10 or higher

Authentication App


TOTP Hardware Token

FIDO Security Key

UCM6308A CloudUCM SoftwareUCM GCC6000 Series

Firmware 1.0.11.10 or higher Firmware 1.0.25.13 or higher Firmware 1.0.27.13 or higher  
Firmware 1.0.7.5 or higher

## Documents / Resources

|   |   |
|---|---|
|  | <p><a href="#">GRANDSTREAM UCM63xx series IP-PBX Multi-Factor Authentication [pdf]</a> User Guide</p> <p>UCM63xx series, CloudUCM, SoftwareUCM, GCC6000 Series, UCM63xx series IP-PBX Multi-Factor Authentication, UCM63xx series, IP-PBX Multi-Factor Authentication, Multi-Factor Authentication, Factor Authentication</p> |
|---|---|

## References

- [User Manual](#)

■ GRANDSTREAM  
🔗 CloudUCM, Factor Authentication, GCC6000 Series, GRANDSTREAM, IP-PBX Multi Factor Authentication, Multi Factor Authentication, SoftwareUCM, UCM63xx Series, UCM63xx series IP-PBX Multi-Factor Authentication

---

## Leave a comment

Your email address will not be published. Required fields are marked \*

Comment \*

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search

[Manuals+](#) | [Upload](#) | [Deep Search](#) | [Privacy Policy](#) | [@manuals.plus](#) | [YouTube](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.