

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 IP-PBX. 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 to 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

	Virtual MFA Device	Physical MFA Device	
Device	See Virtual MFA Applications table below	TOTP Hardware Token	FIDO Security Key
Cost	Free	Price determined by 3rd party vendor	Price determined by 3rd party vendor
Device Specifications	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.
Application Scenario	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	Google Authenticator Twilio Authy 2-factor Authentication
iOS™ Mobile Devices	Google Authenticator Twilio Authy 2-factor Authentication
Windows™ Mobile Devices	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

[Email Settings](#)
[Email Template](#)
[Email Footer Hyperlink](#)
[Email Send Log](#)

TLS Enable

☒

Type

Client

Email Template Sending Format

HTML

Mail Server Domain

mycompany.com

* SMTP Server

192.168.56.20:7006

Enable SASL Authentication

☒

* Username

pbx1mail@mycompany.com

ⓘ

The email server must allow 3rd party email clients to use the SMTP service.

* Password

.....

Enable Email-to-Fax

☐

* Display Name

PBX

* Sender

pbx1mail@mycompany.com

Cancel

Save

Email Settings

- 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 Management > Edit User Information: admin

* Username

admin

Privilege

Super Administrator

User Password

[Change Password](#)

* Email Address

Arthur.Morgan@mycompany.com

Mobile Number

+1

Multi-Factor Authentication

☐

[Instructions](#)

Cancel

Save

User Information

- 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

01

Install the application in your phone or computer.
[View Compatible Applications List](#)

02

Scan the QR code with your software token application, or enter the Secret Key.

Show QR Code

OR

Show Secret Key

03

Enter the first MFA code on the application

04

Enter the second MFA code that appears after the first expires

Previous

OK

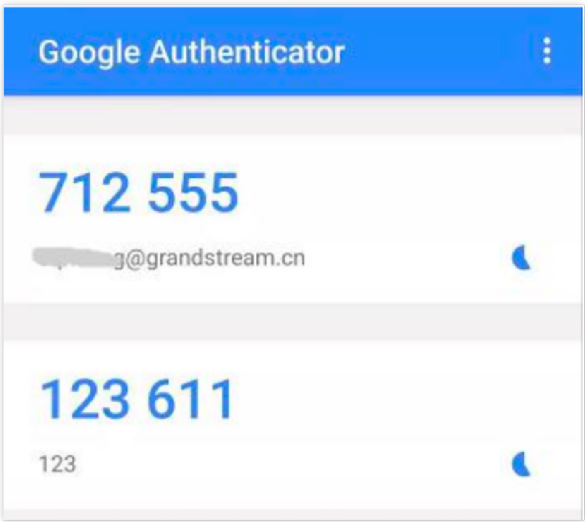
Authentication App Instructions

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

01

Enter the secret key received from the hardware key manufacturer. [How to obtain](#)

02

Press the button on the device and enter the 6-digit code.

03

Wait 30 seconds and then press the button to enter the new 6-digit code displayed on it.

Previous

OK

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.

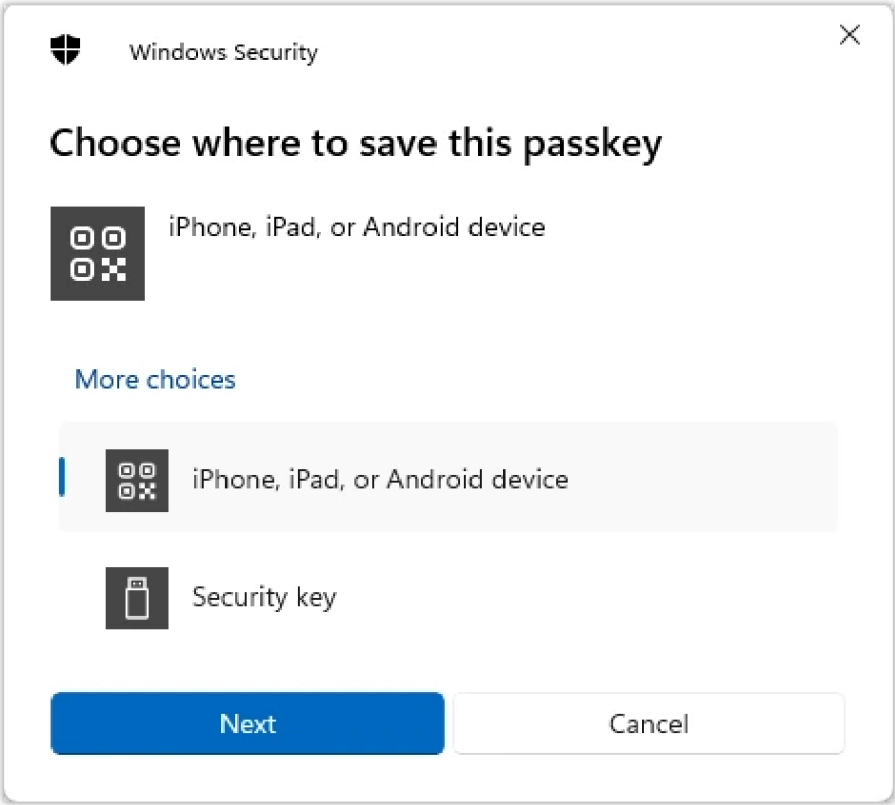
 Notes

- 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 Settings**→**Email 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 **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 **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.

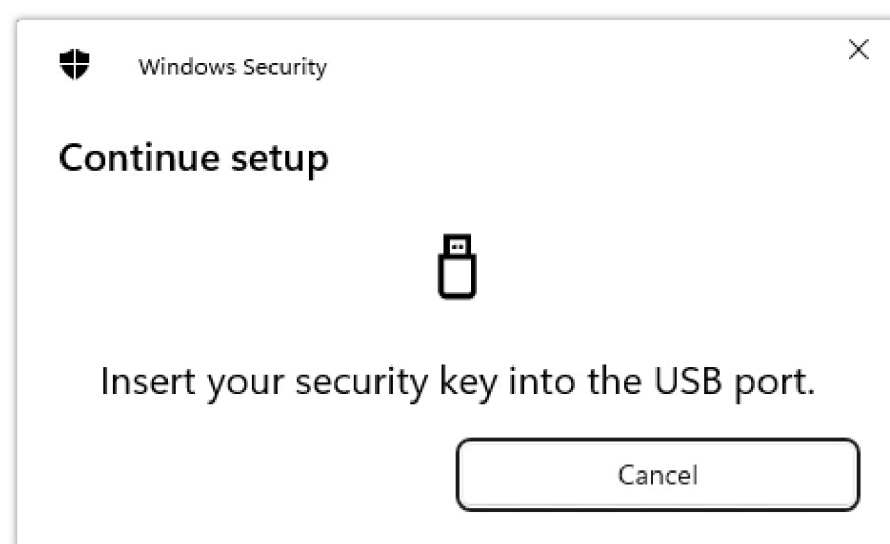


Storage Method for FIDO Passkey

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.

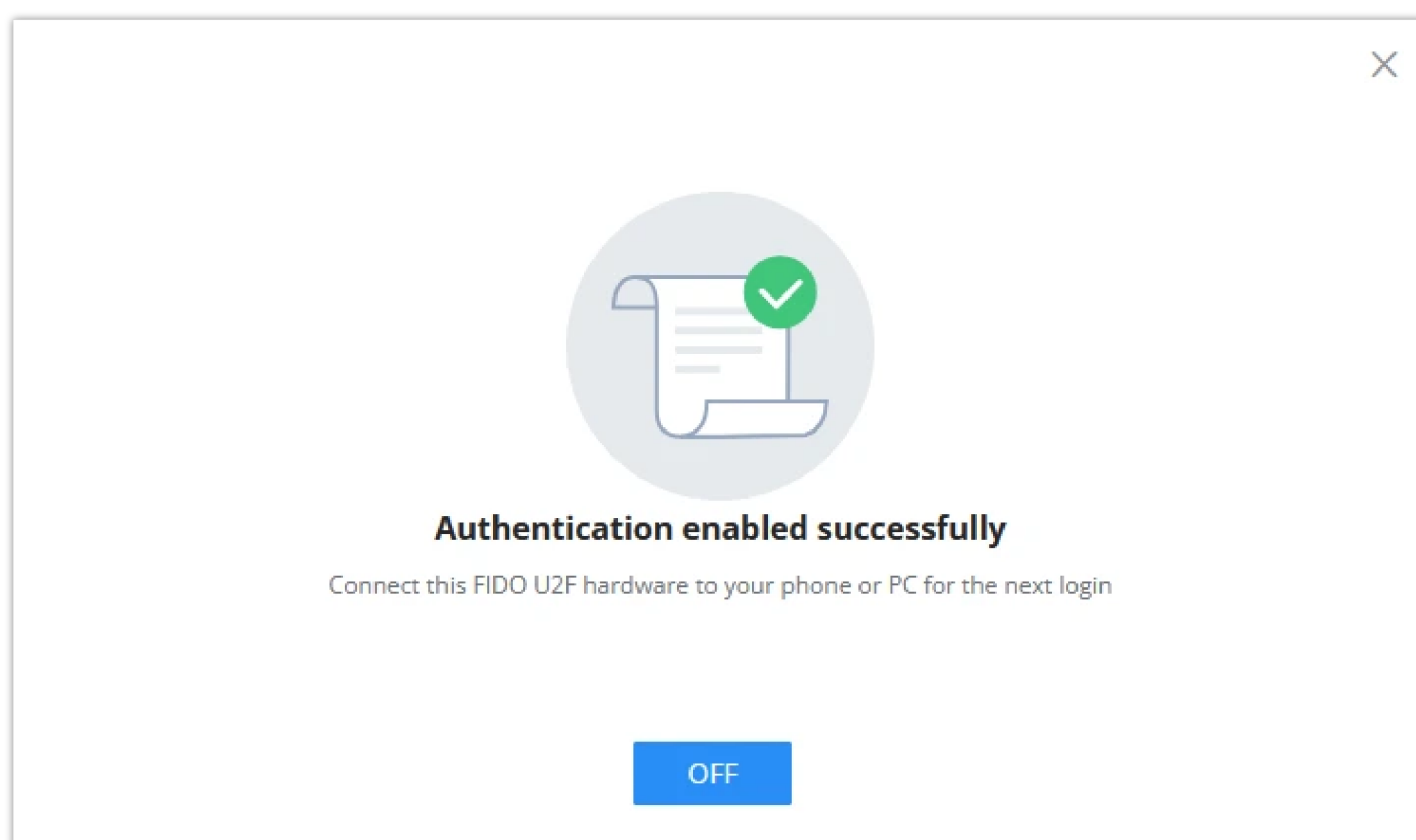


Saving Passkey on iPhone, iPad, or Android Device



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	Minimum Firmware Version	Authentication App	TOTP Hardware Token	FIDO Security Key
UCM6301	Firmware 1.0.11.10 or higher	✓	✓	✗
UCM6302	Firmware 1.0.11.10 or higher	✓	✓	✗
UCM6304	Firmware 1.0.11.10 or higher	✓	✓	✗
UCM6308	Firmware 1.0.11.10 or higher	✓	✓	✗
UCM6300A	Firmware 1.0.11.10 or higher	✓	✓	✗
UCM6302A	Firmware 1.0.11.10 or higher	✓	✓	✗
UCM6304A	Firmware 1.0.11.10 or higher	✓	✓	✗

UCM6308A	Firmware 1.0.11.10 or higher	✓	✓	✗
CloudUCM	Firmware 1.0.25.13 or higher	✓	✓	✓
SoftwareUCM	Firmware 1.0.27.13 or higher	✓	✓	✗
GCC6000 Series	Firmware 1.0.7.5 or higher	✓	✓	✗

