UCM6xxx Security Manual

This document presents a summary of security measures, factors, and configurations that users are recommended to consider when deploying the UCM.

> We recommend to always use the latest official firmware for improved security.

The following sections are covered in this document:

- **Web UI Access**

Web UI access is protected by username/password and login timeout. Two-level user management is configurable. Admin with limited access can be created by the default super administrator.

- **Extension Security**

Extension security utilizes SIP/IAX passwords for authentication, SRTP and ZRTP encryption for SIP calls.

- **Trunk Security**

Trunk security utilizes privilege levels and source caller ID filters to prevent outbound calls from unintended sources.

- **TLS Protocol**

TLS is utilized to encrypt SIP signaling.

- **Firewall Features**

Three different security measures can be configured to protect the UCM against malicious attacks: Static Defense, Dynamic Defense and Fail2ban.

- **AMI**

AMI feature is used to let the user connect to Asterisk instance to read and track the state of telephony client, it may come with security concerns for UCM administrators that needs to be considered.

Web UI Access

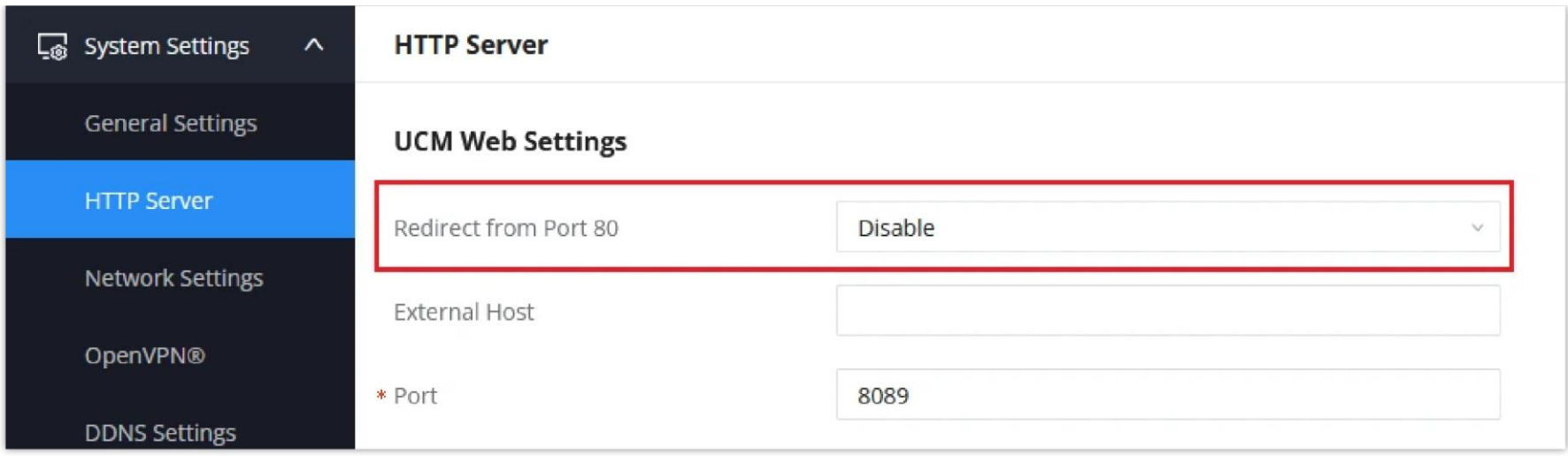
UCM HTTP Server Access

The UCM embedded web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a web browser such as Microsoft Edge, Mozilla Firefox, Google Chrome, etc. With this, administrators can access and configure all available UCM information and settings. It is critical to understand the security risks involved when placing the UCM on public networks.

Protocol Type

Grandstream IPPBXs only support HTTPS protocol for web access. To secure transactions and prevent unauthorized access, it is highly recommended to:

1. Disable option Redirect from Port 80 and,
2. Avoid using well known port numbers such as 80 and 443.

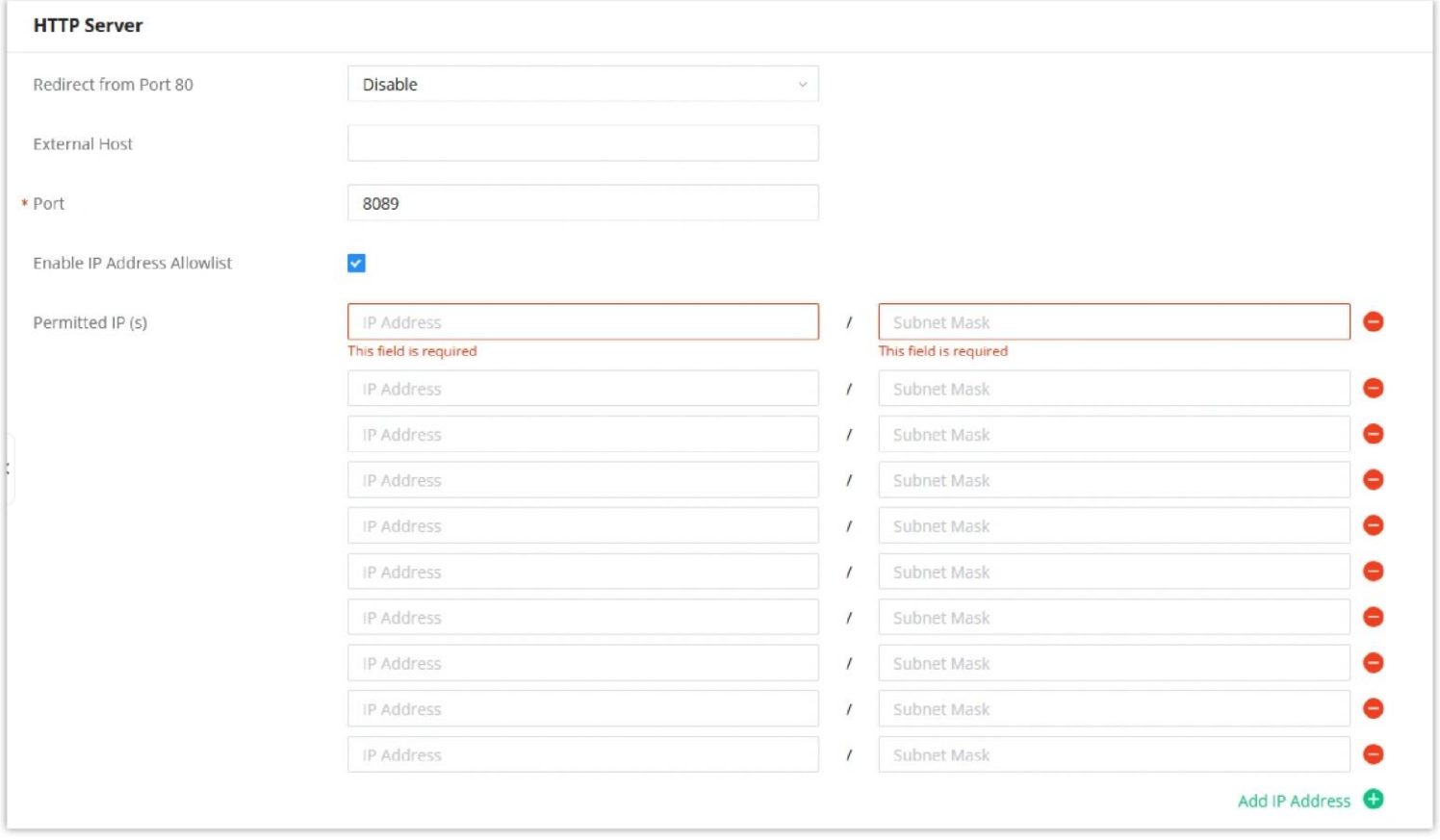


HTTP server settings in UCM63xxA series

Finally, users have the option to specify a list of up to 10 IP addresses which will be allowed to access the UCM web UI. Addresses not listed will be restricted from accessing the UCM.

To enable and add to the IP address whitelist, navigate to **System Settings > HTTP Server**:

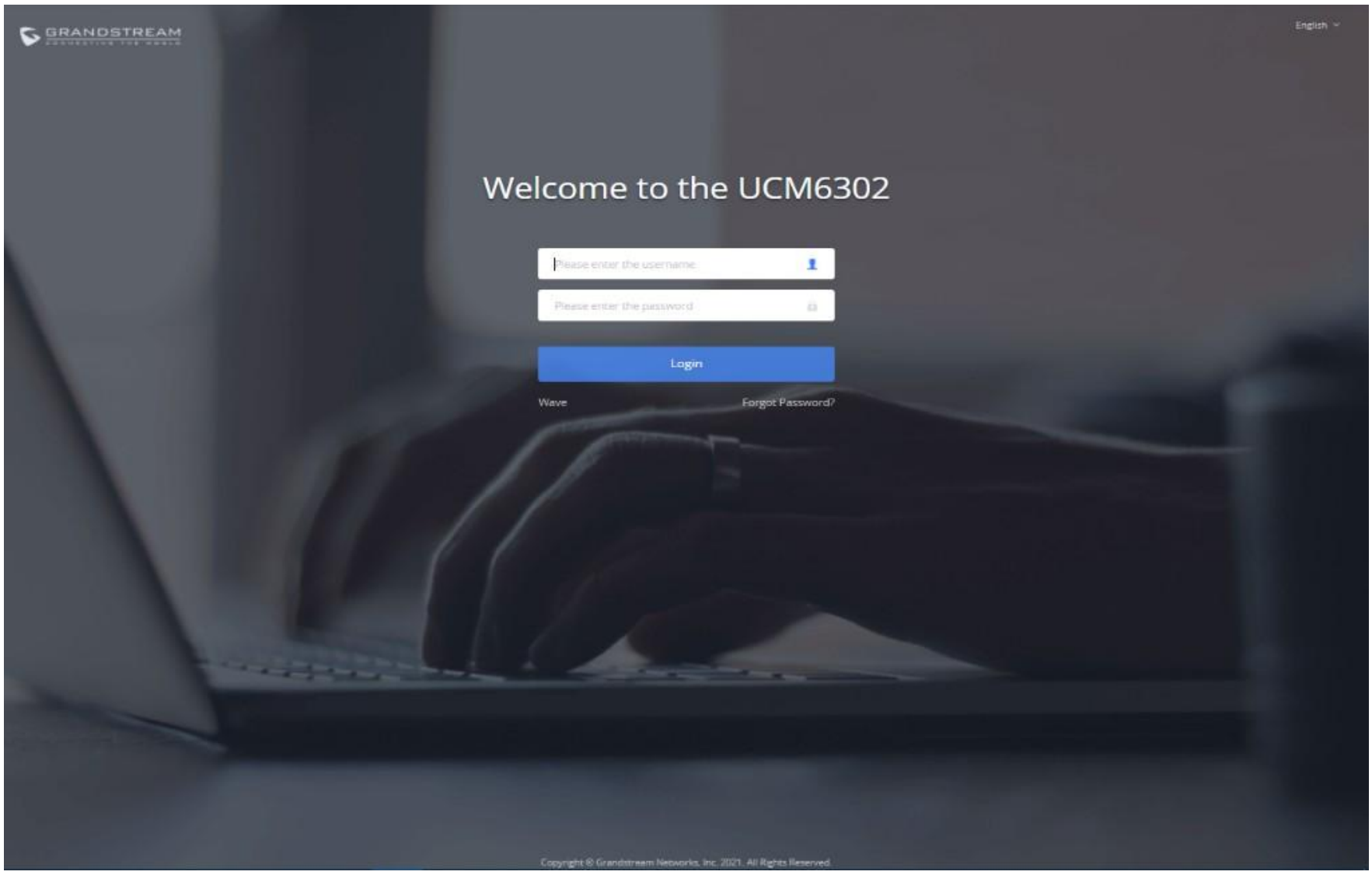
- Check the option “Enable IP Address Whitelist”
- Enter the permitted IP addresses along with the subnet masks.



IP address whitelist to access the UCM

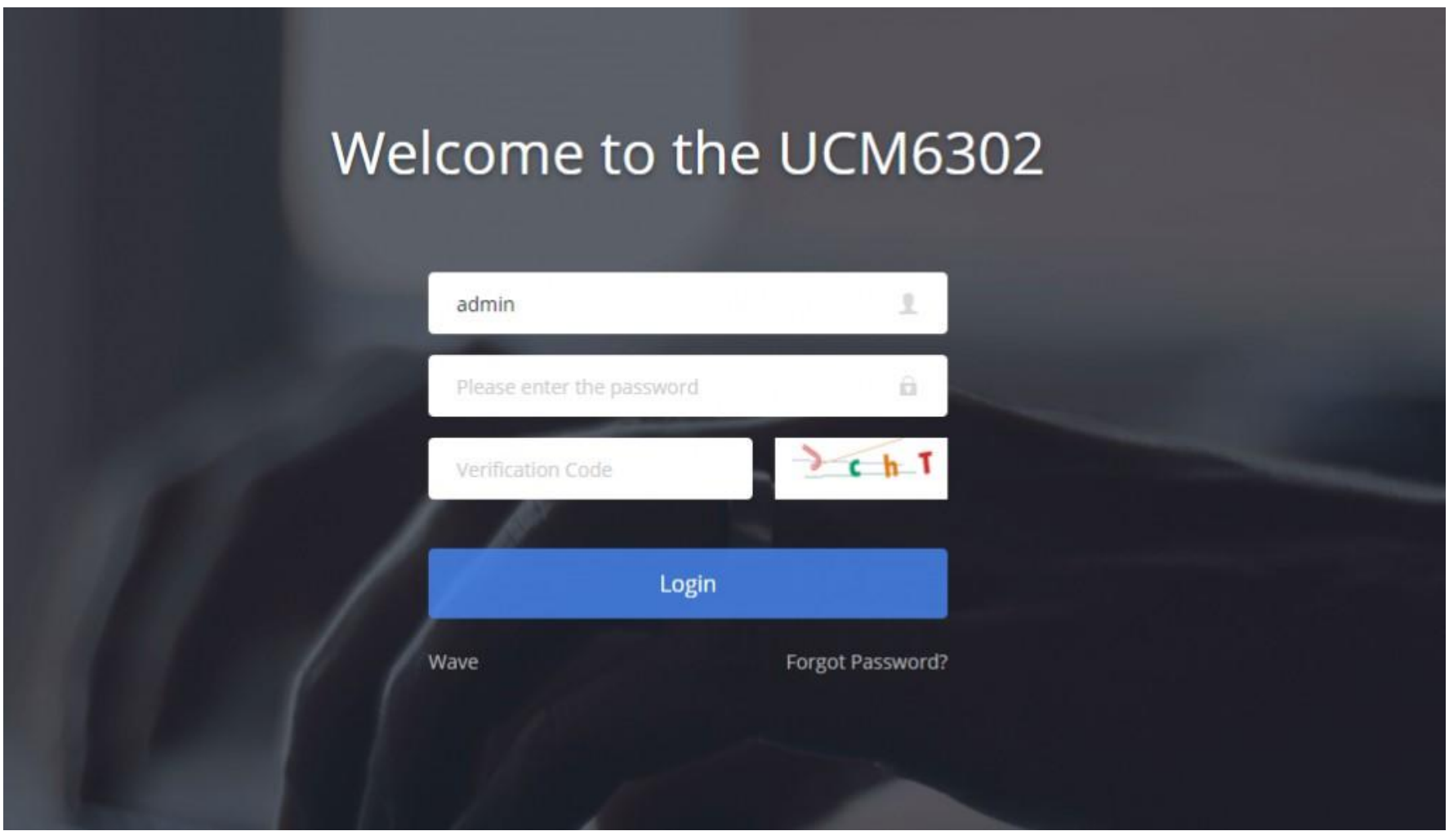
User Login

Username and password are required to log into and access the UCM web UI.



UCM6302 Web UI Login

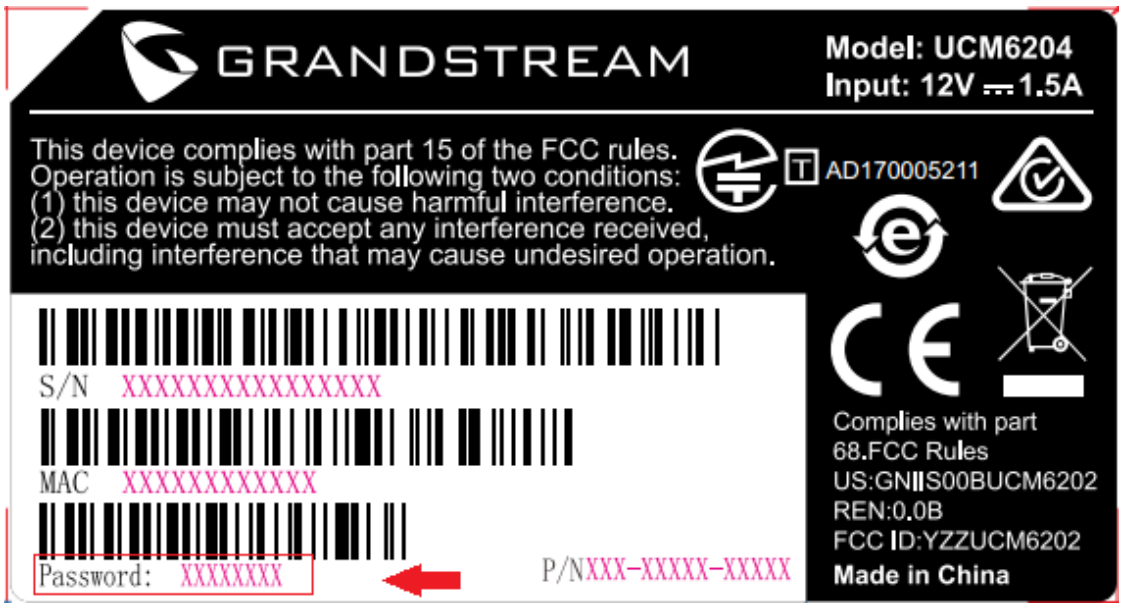
In case the user enters a wrong username or password, the user will have to enter a captcha verification in order to log into the UCM. This secures the UCM from automated attempts to log in.



Captcha Verification

The factory default username is “admin” while the default random password can be found on the sticker at the back of the unit.

Note: Units manufactured starting January 2017 have a unique random password printed on the sticker.



Default Random Password

It is highly recommended to change the password after logging in for the first time.

To change the password for default user "admin", navigate to **Maintenance→Login Settings→Change Password**. The password length must be between 10-30 characters.

If **PBX Settings→General Settings→Enable Strong Password** is toggled on, the password must contain at least one of each of the following:

- Uppercase letters.
- Lowercase letters.
- Numbers.
- Special characters.

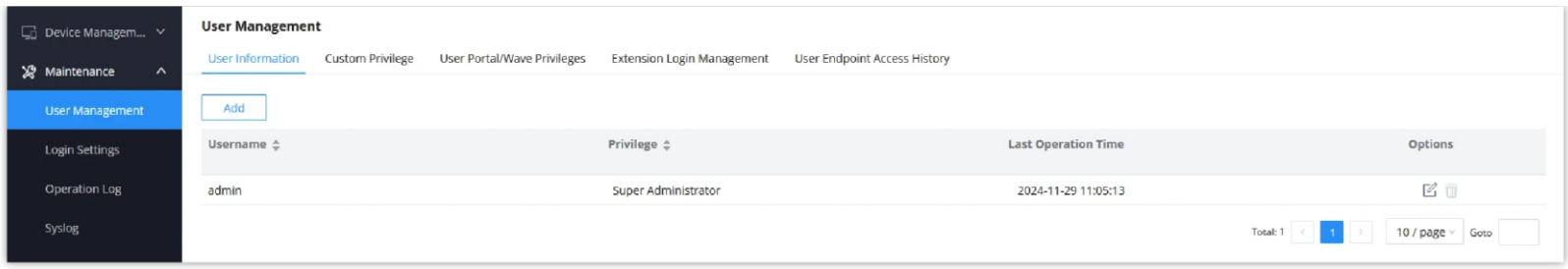
Strong passwords with a combination of numbers, uppercase letters, lowercase letters, and special characters are always recommended for security.

Multi-factor Authentication (MFA)

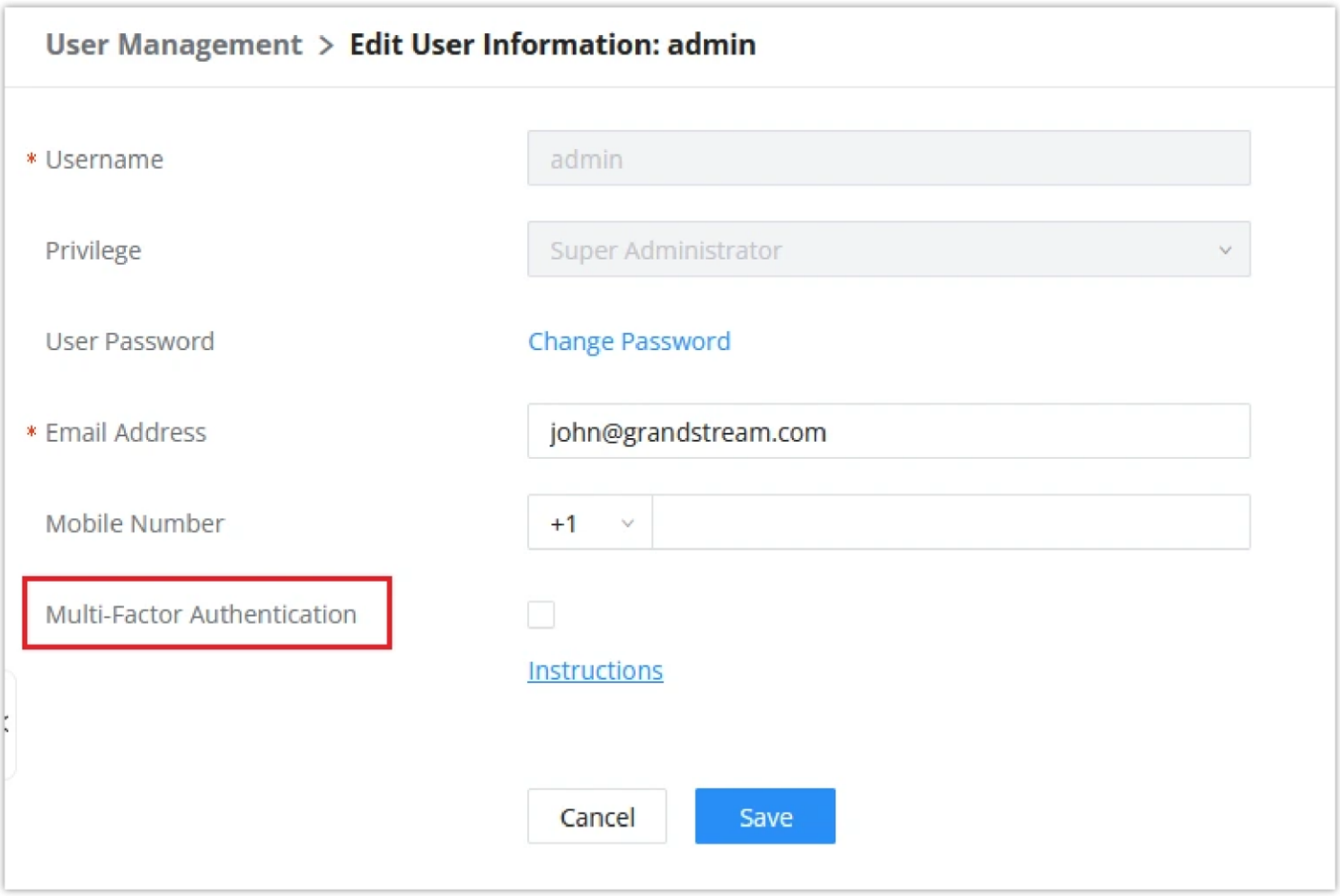
The UCM supports the multi-factor authentication feature that adds a layer of security by presenting a one-time password (OTP) that is generated by either a physical device or a virtual generator, like Google Authenticator app that can be installed on both Android™ and iOS™ mobile phone. It's worth to note that the UCM supports only Google Authenticator, Twilio Authy 2-Factor Authentication (Android™ and iOS™) as a virtual code generators and Microcosm physical OTP devices. Grandstream has chosen this policy to ensure the highest level of security.

> **Important**
>
> Before you can be able to configure this feature, you must configure the email settings under System Settings. This is the only way to disable the MFA feature in case of loss of your virtual or physical MFA device.

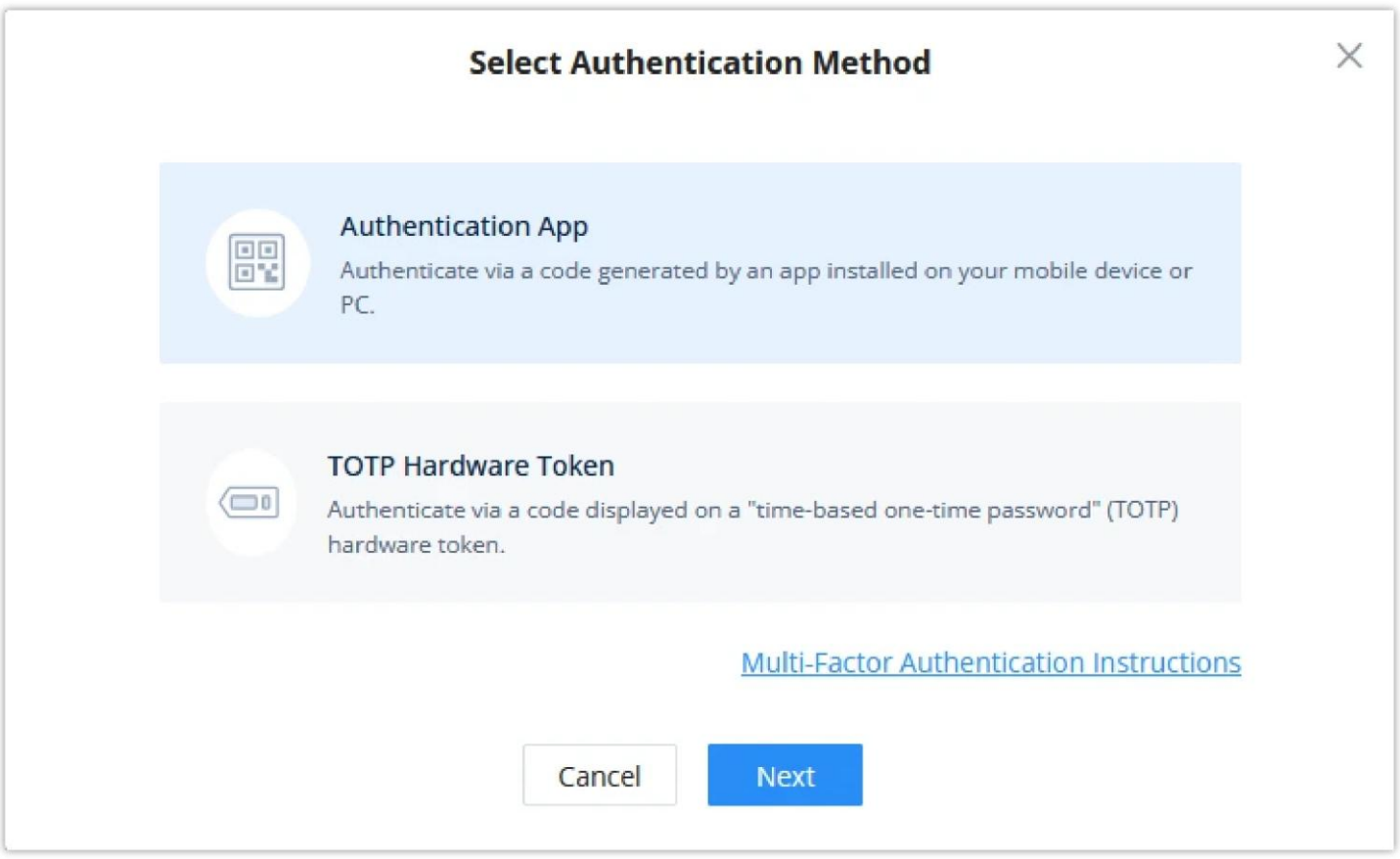
To enable this feature please navigate to **Maintenance > User Management**



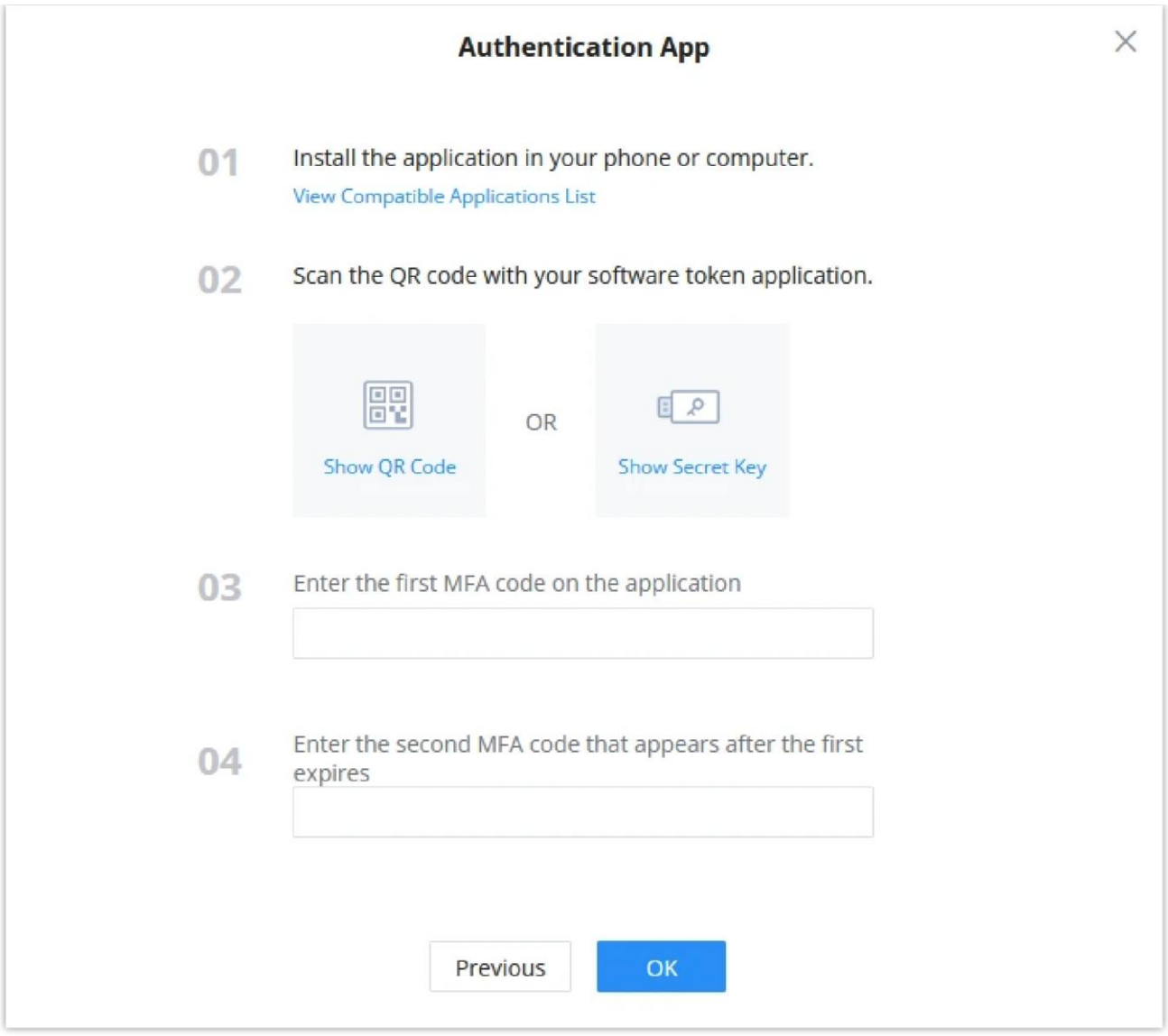
Then click on the edit button and enable “Multi-Factor Authentication” feature as shown in the screenshot down below:



Then choose the type of MFA. If you already have a physical MFA device, choose “TOTP Hardware Token”. If you want to use virtual MFA instead, choose “Authentication App”:



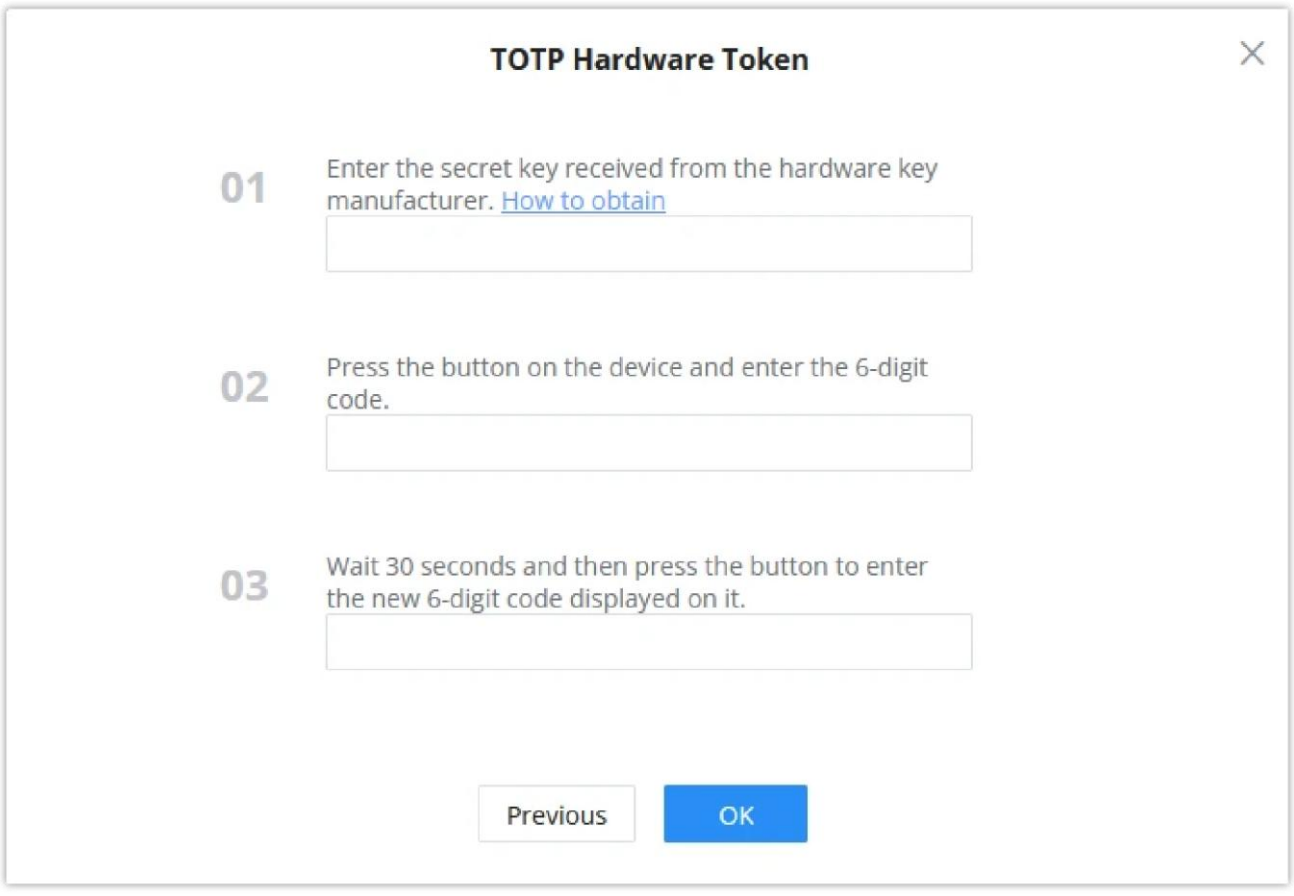
Press *“Next”*. In case you have selected “Authentication App” you’ll encounter this window:



Click on “View Compatible Applications List” to find the links to download the supported apps, then install the application that’s compatible with your smartphone OS.

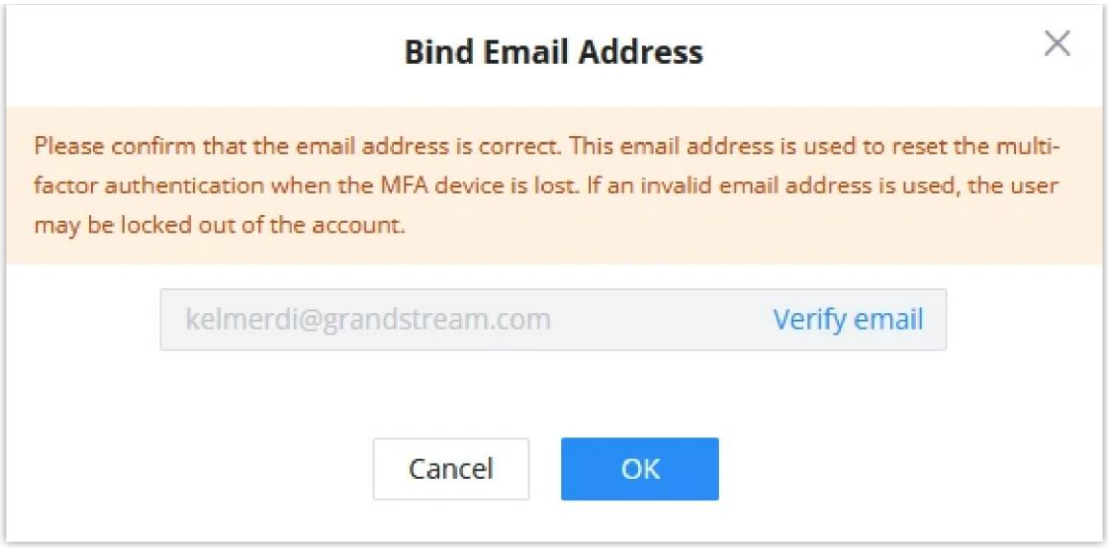
Once installed, open the app and scan the QR code to set up the codes. Enter the first code in the “Code1” text area, then wait until it expires and enter the new code in “Code2” text area. After that click on **OK**.

In case you have chosen to use physical MFA devices, this prompt will appear:



Fairly similar to virtual MFA device configuration, you will have to enter a key that the manufacturer of your MFA devices would have provided with the devices, then enter follow the instructions in the prompt. Click **OK** when both codes are entered.

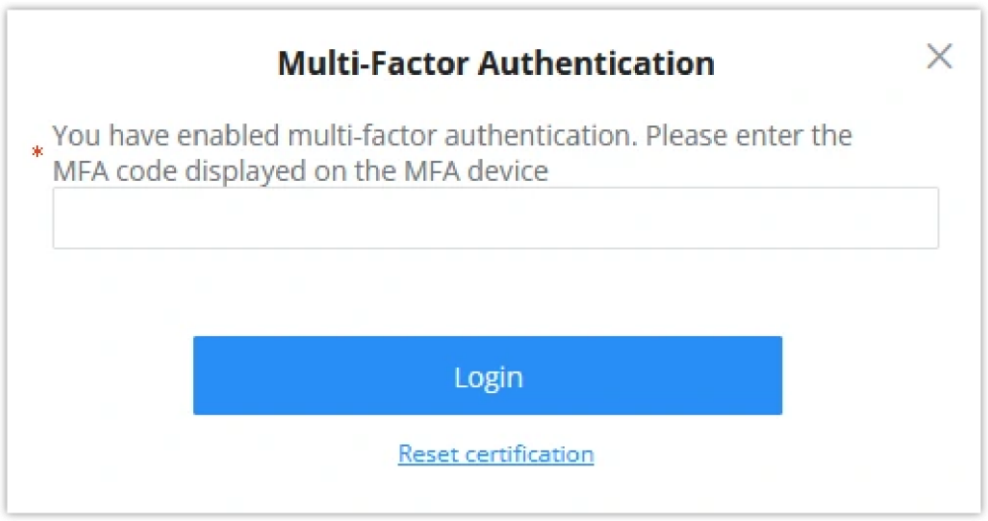
In either cases, this prompt will appear while you save the settings in the UCM:



This step is very important as it shows the email that you will use to disable Multi-factor Authentication in case you have lost your physical MFA device or your mobile phone which has the virtual MFA device installed on.

Click **OK** and the UCM will send a test email to your email address to verify if the email settings are set correctly. Then click *"Apply Changes"*.

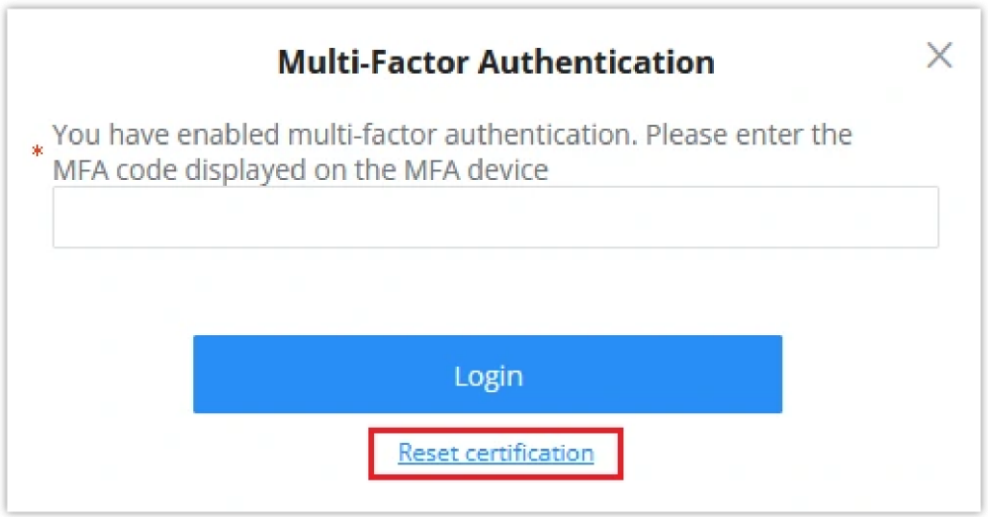
To test if MFA has been set correctly, log out from the UCM then try to log in again. After you have entered the correct username and password, this page will appear where you will have to enter your code (One Time Password) that is shown on the authenticator application or on your MFA physical device:



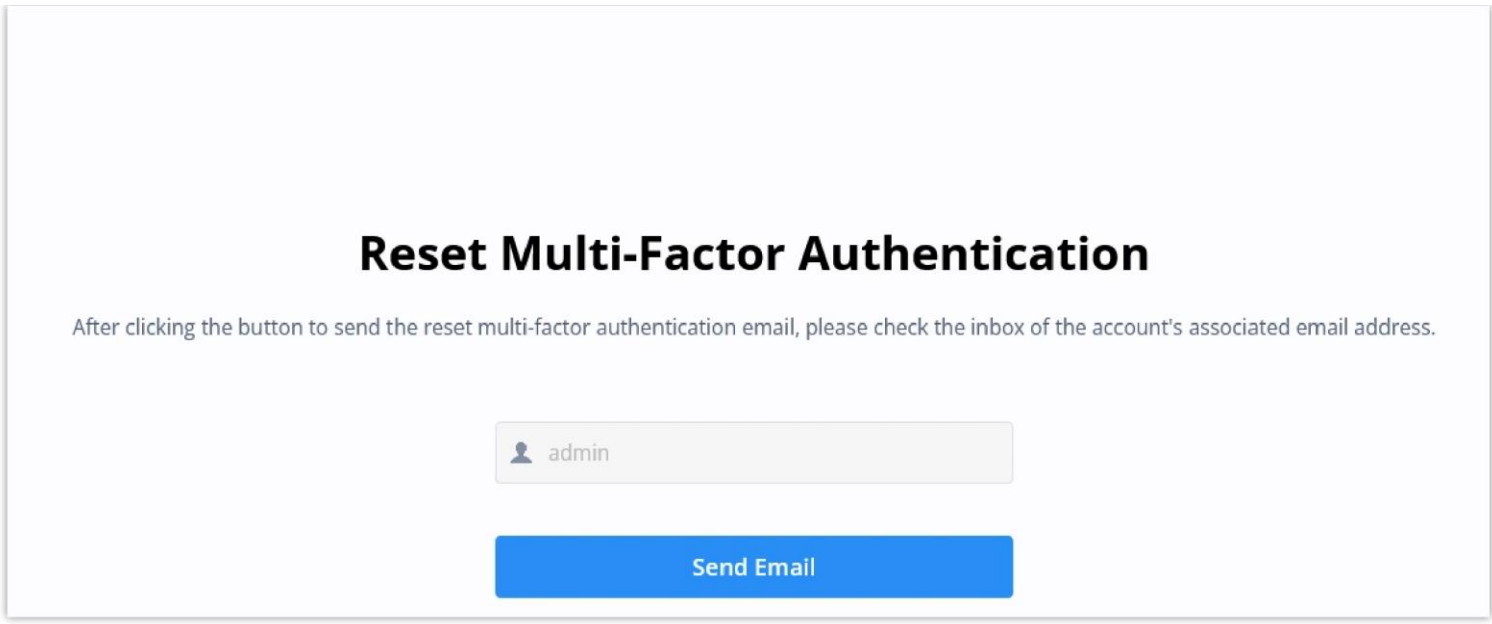
Reset Multi-factor Authentication Certifications

In case you have lost your MFA device, whether physical or virtual, you can easily disable MFA for your UCM account through the email address that is set with your UCM account.

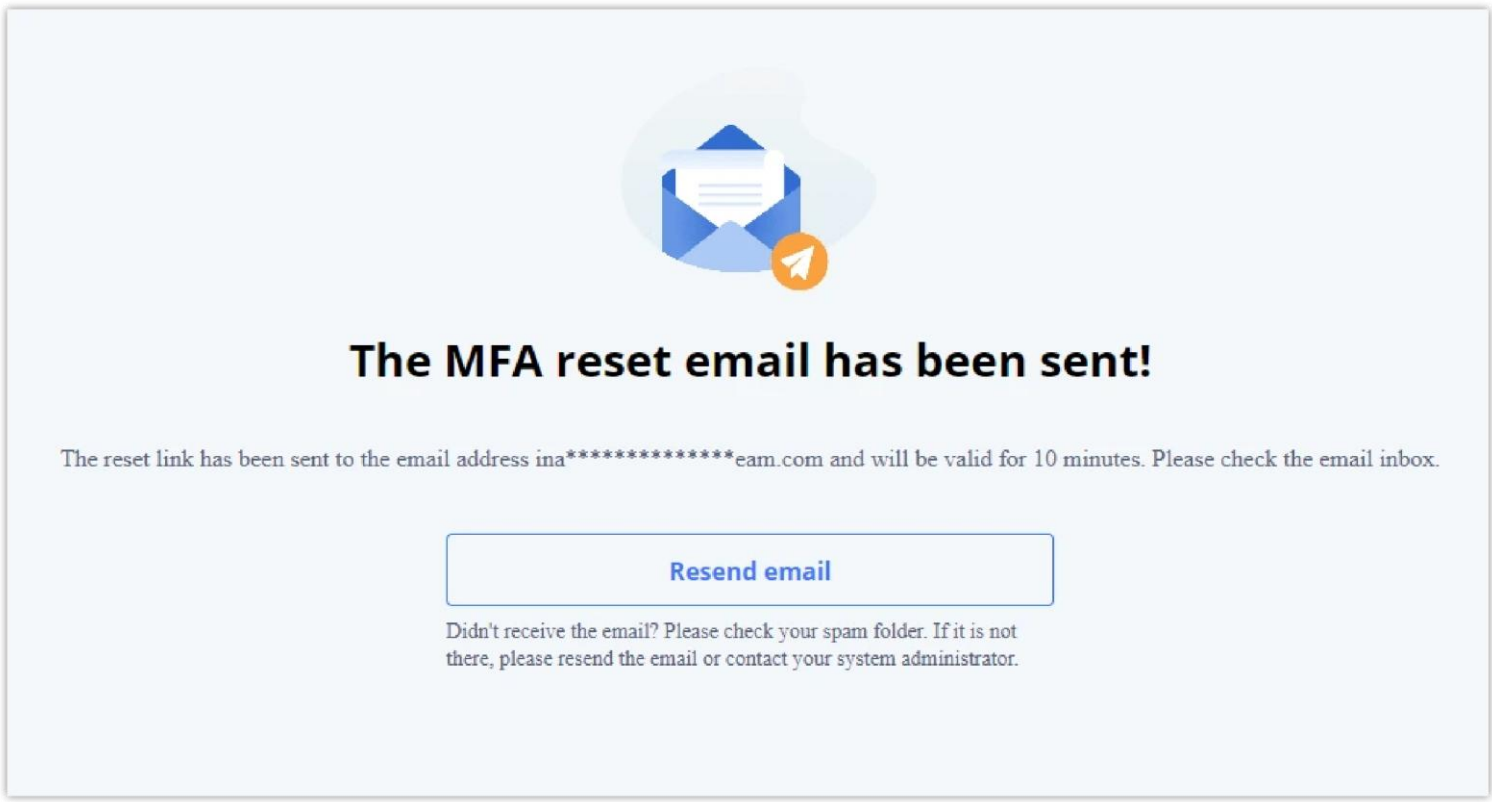
To do this, log into the UCM with your credentials and when you are prompted to enter the MFA code, click on "Reset certification" as shown in the screenshot down below:



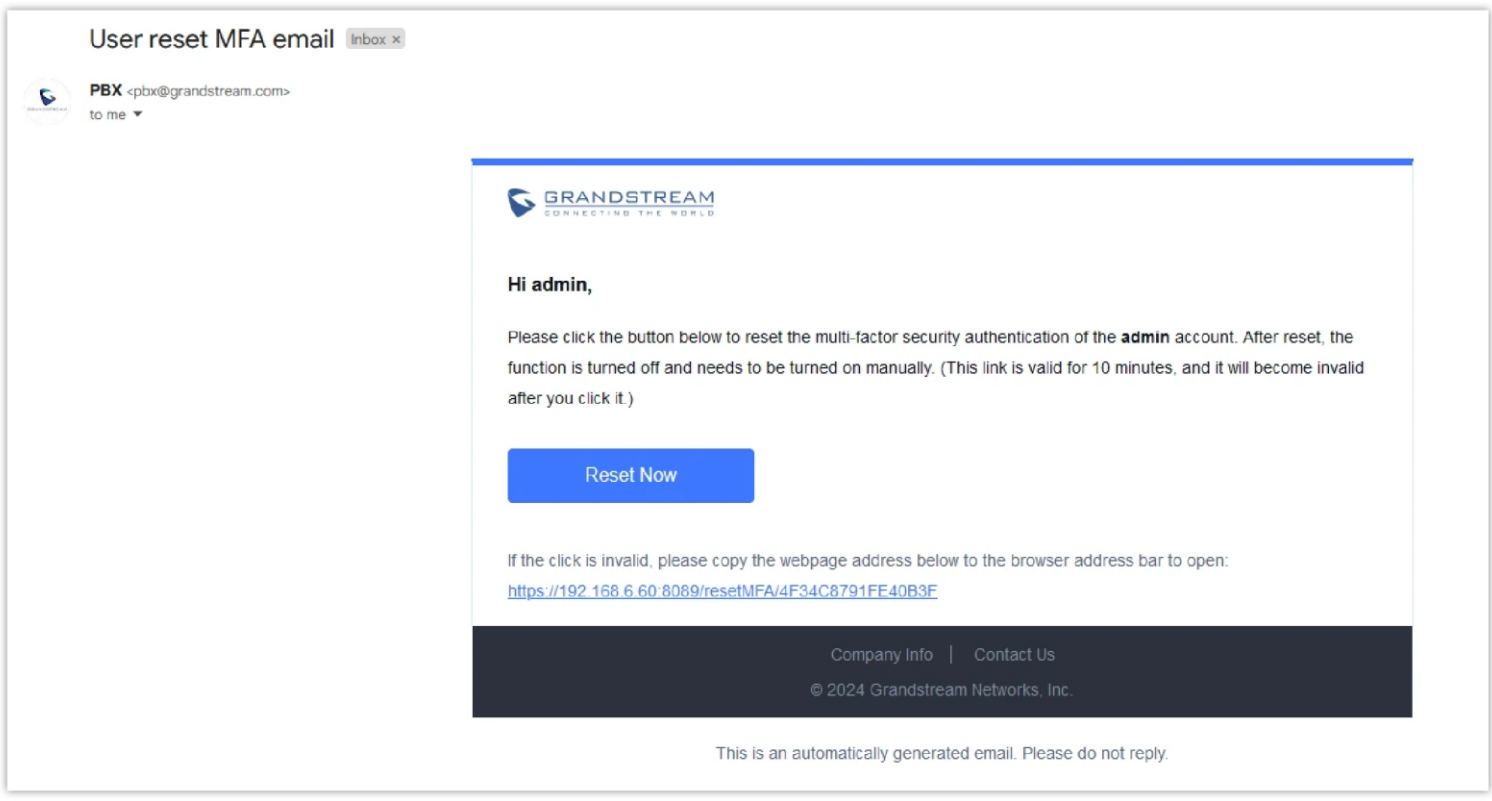
This message will appear:



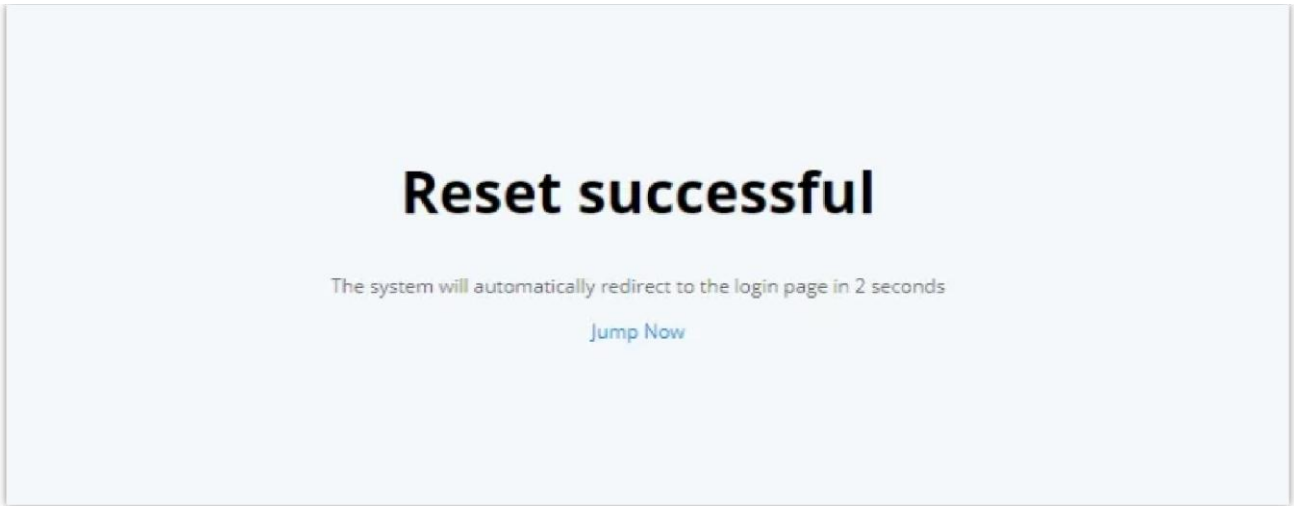
Click on *"Send Email"*. The UCM will confirm that the email containing the link to reset the MFA has been sent



On your email box, you will receive an email that looks similar to this one:



Click on *"Reset Now"*. This message will appear and you'll be automatically redirected to UCM's log in web page to log in without having to enter the MFA code.

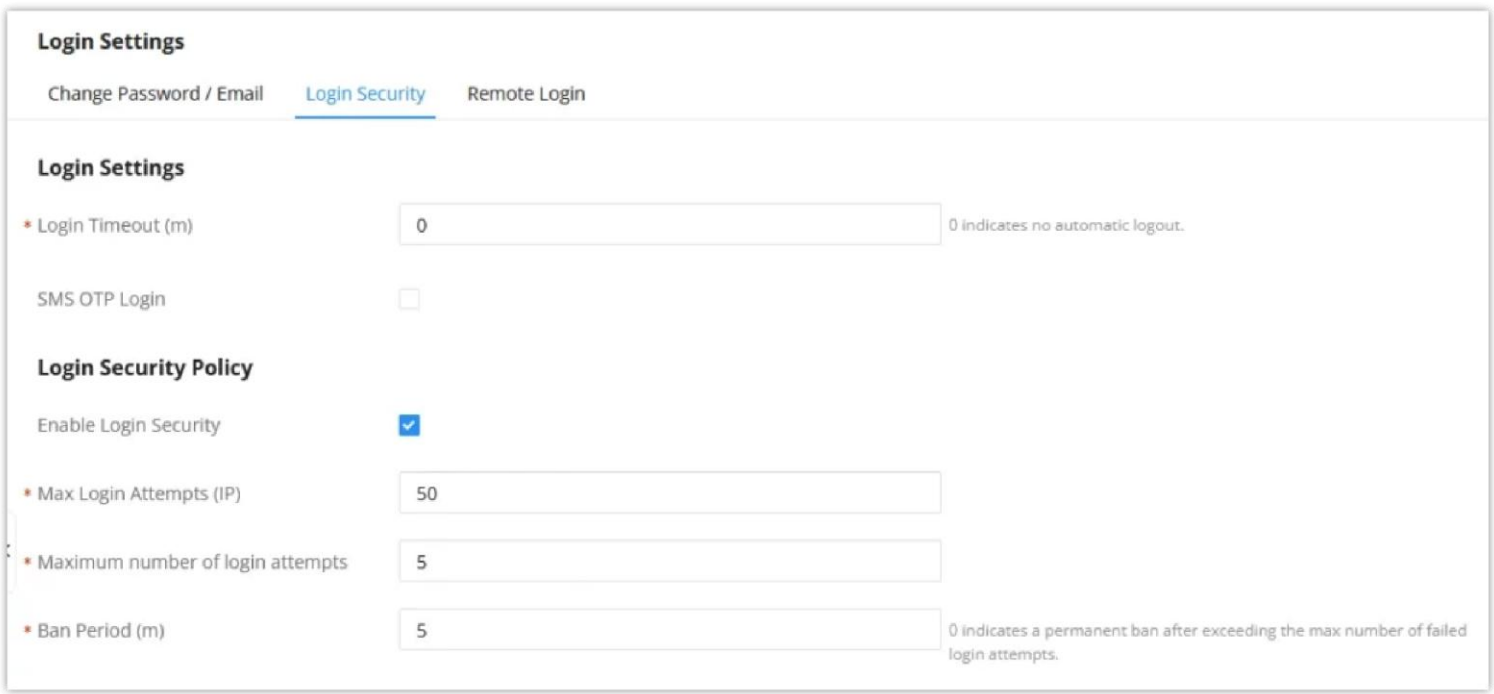


Login Settings

To further prevent unauthorized access to the UCM web UI, users will automatically be logged out after the configured period of inactivity. Username and password will be required to access the web UI again.

The default login timeout is 10 minutes and can be changed by navigating to **Maintenance > Login Settings > Login Security** and modifying the User Login Timeout field.

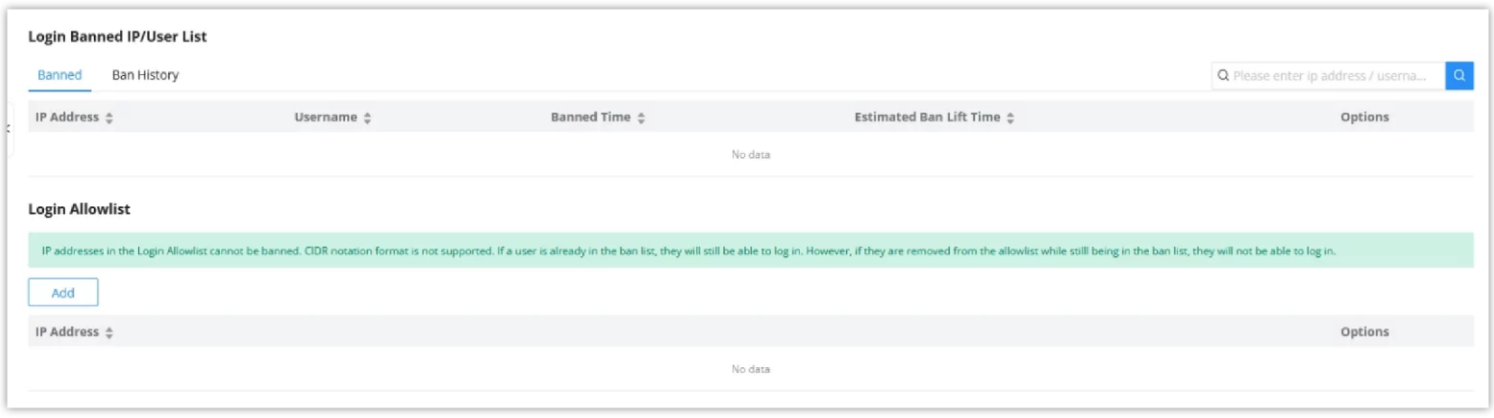
Additionally, the UCM can also ban users after a specified number of failed login attempts for a specified amount of time. By default, users will be banned for 5 minutes after 5 failed login attempts.



Login Settings

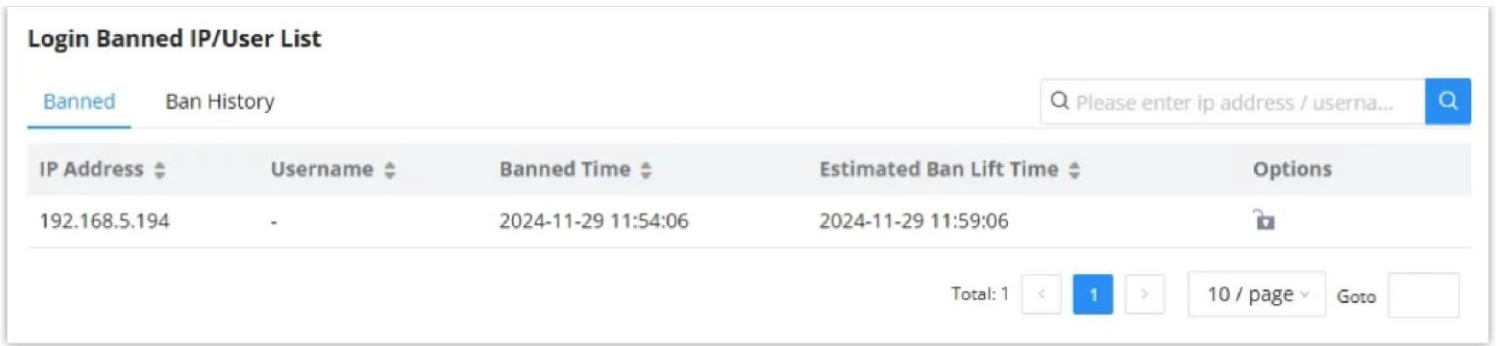
If a user exceeds the Max Login Attempts (IP) limit, their IP will be banned from accessing the UCM. The ban will be permanent if the Ban Period (m) is set to 0, or temporary for the duration specified in the Ban Period (m).

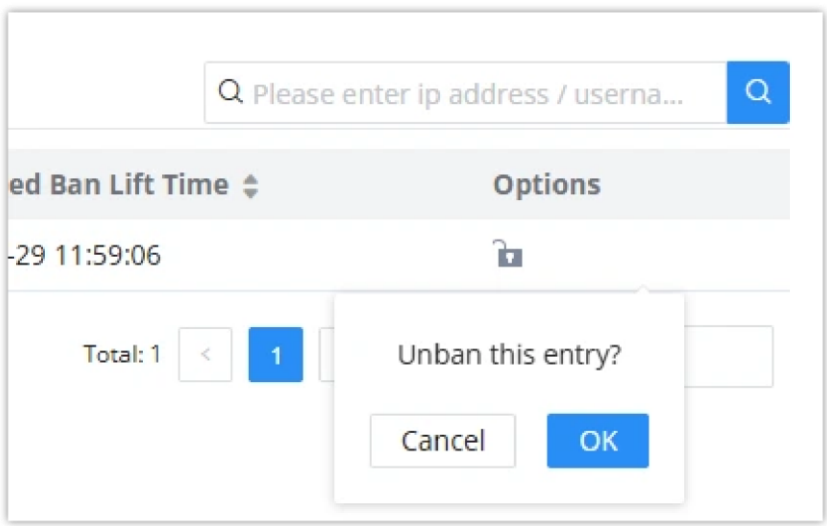
Users can unban specific IPs listed in the **Login Banned IP/User List**. They can also add IP addresses to the **Login Allowlist**, preventing them from being banned.



IP Login Ban and Allow List

To unban an IP, please click the lock icon under **Options** and select **OK** to confirm the action .





User Management Levels

Four user privilege levels are currently supported:

- **Super Admin**
- **Admin**
- **Custom level**

Super Admin has access to all of the UCM's pages and can execute any operation. Admin can access most of the UCM's pages with the exception of the following:

- **Maintenance > Upgrade**
- **Maintenance > Backup**
- **Maintenance > System Cleanup/Reset**
- **Maintenance > Operation Log**

A "Super Admin" user with username "admin" is initially configured on the UCM with factory settings. It is the only allowed "Super Admin" account and cannot be deleted and changed. This super administrator could create, edit and delete new user accounts with lower privileges "Admin" and "Custom".

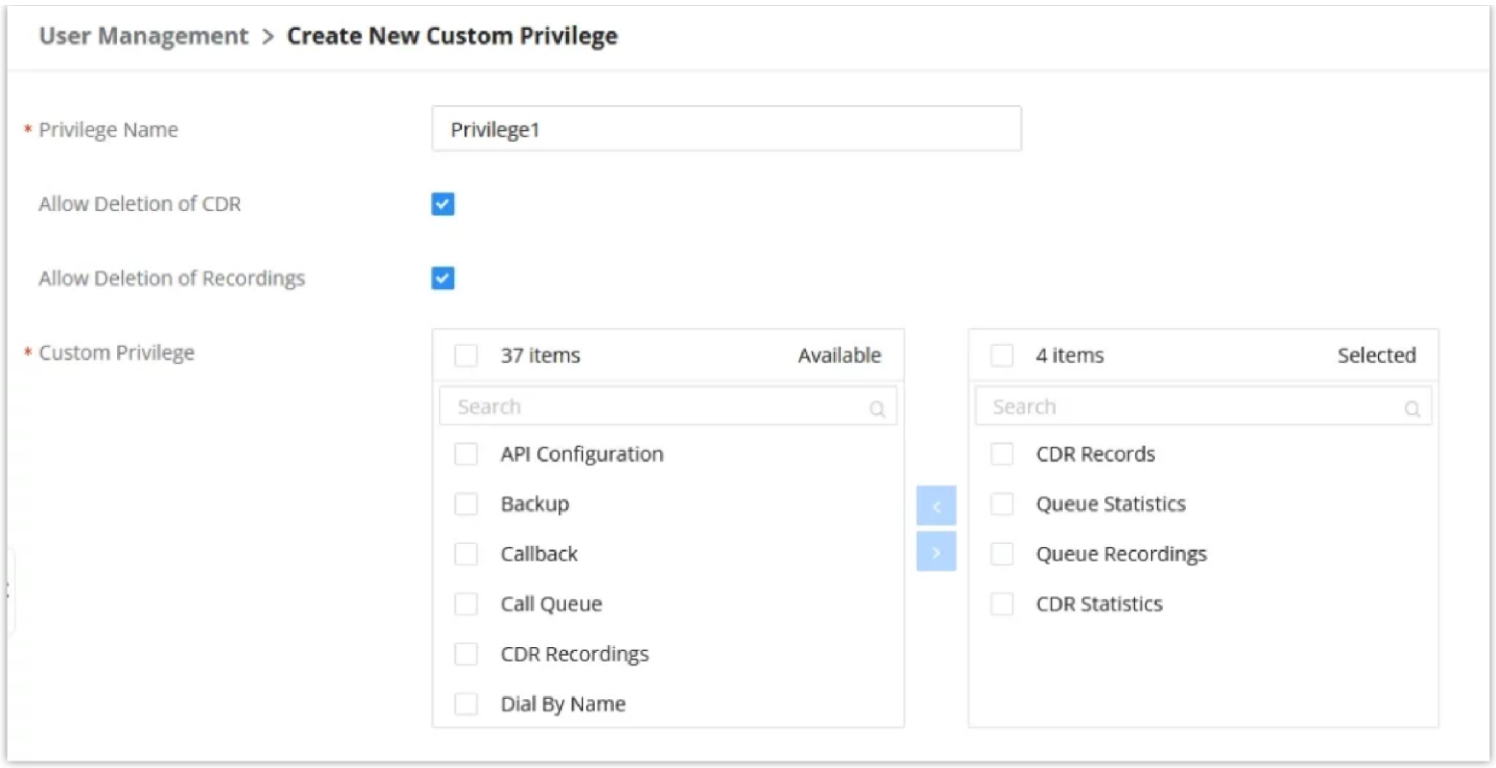
Only Super Admin has the authority to view the activity of all users via the Operation Log.

If there is more than one PBX administrator managing the UCM, it is highly recommended to create Admin level users instead of giving out Super Admin access.

Custom privilege user levels can also be created and modified to have specific permissions including but not limited to:

- Status
- Conference
- System Events
- Feature Codes
- CDR
- PMS-Wakeup Service

To create a new custom privilege level, navigate to **Maintenance→User Management→Custom Privilege**, name the new custom user level and assign the desired modules as shown in the figure below.



Creating Custom Privilege Levels

"Allow Deletion of CDR" and "Allow Deletion of Recordings" options are used to determine if the user with CDR and recording files custom privilege can delete CDR and recording files or not.

Extension Security

SIP/IAX Password

When creating a new SIP/IAX extension, the UCM administrator is required to configure "SIP/IAX Password" which will be used for account registration authentication.

If "Enable Random Password" (**PBX Settings→General Settings**) is enabled, "SIP/IAX Password" is automatically filled with a randomly generated secure password when creating the extension on the UCM.

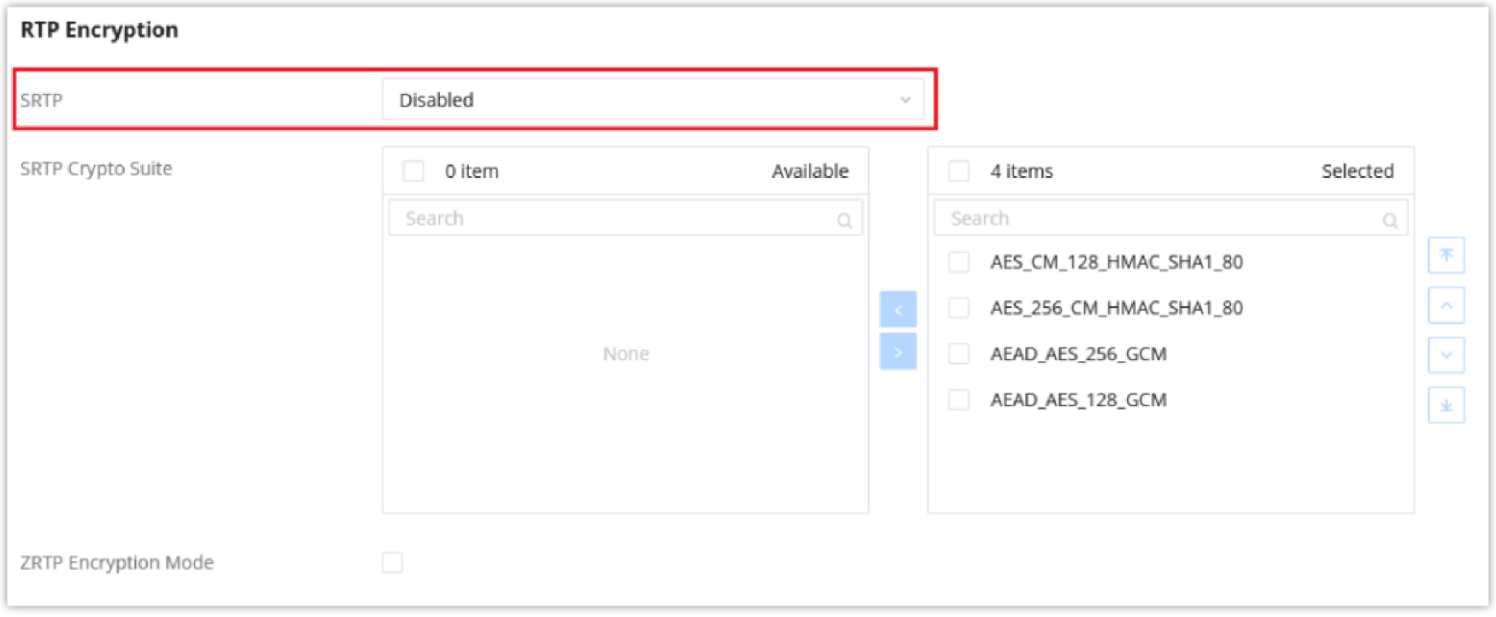
Password Requirements

Passwords must contain 1) at least one number and 2) at least one lowercase letter, uppercase letter, special character and at least 8 characters".

SRTP

UCM supports SRTP for encrypted audio streams. It is disabled by default. To enable it, navigate to **Extensions→Edit Extension→Media→RTP Encryption** and select the desired SRTP option.

Users can select the SRTP encryption suite for outbound calls in UCM, with priority determined by the order of their selection.



Enabling SRTP

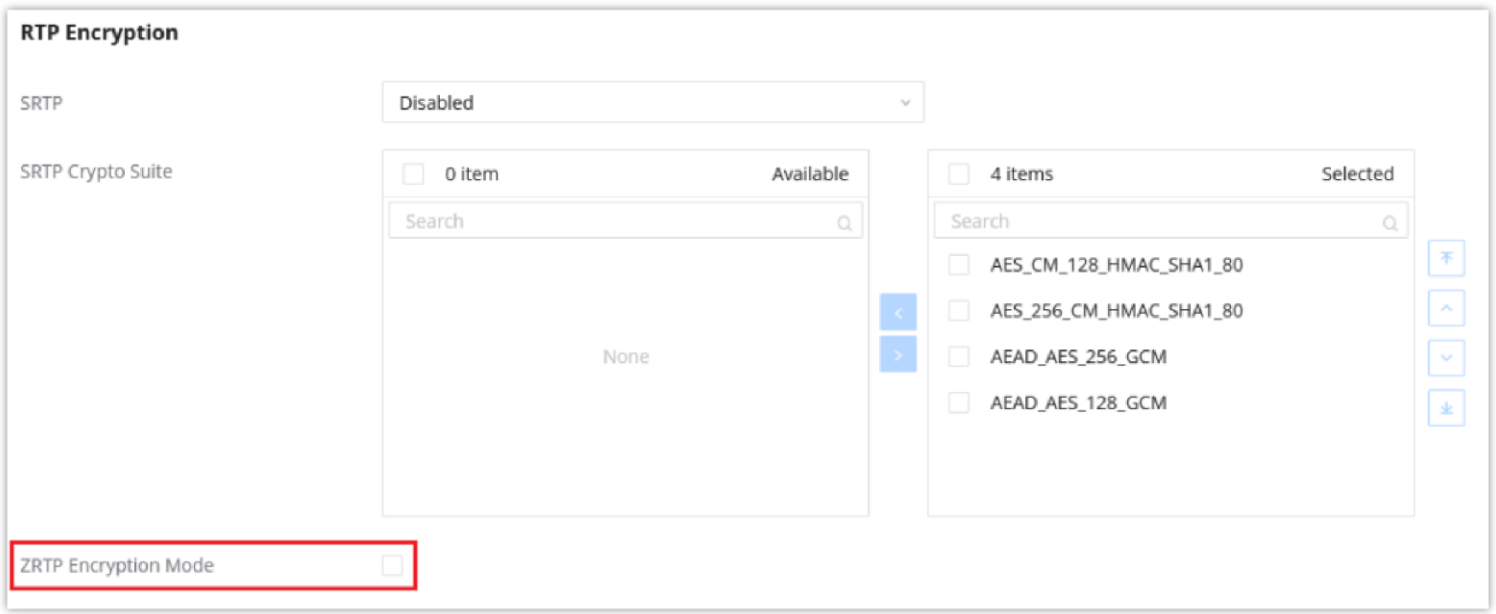
As shown above, users have two options while enabling SRTP under extension parameters:

- **Disabled:** SRTP encryption will be disabled.
- **Enabled and forced:** Extension will support SRTP and will not allow any calls without it.
- **Optional** Extension will support SRTP and will allow negotiation with calls without SRTP.

ZRTP

The UCM63xx series supports ZRTP to establish an encrypted and secure connection between the PBX and the SIP endpoint. It can be enabled from **Extensions→Edit Extension→Media→RTP Encryption**.

> **Note:**
>
> If the SIP endpoint has both SRTP and ZRTP enabled, ZRTP will always be prioritized.



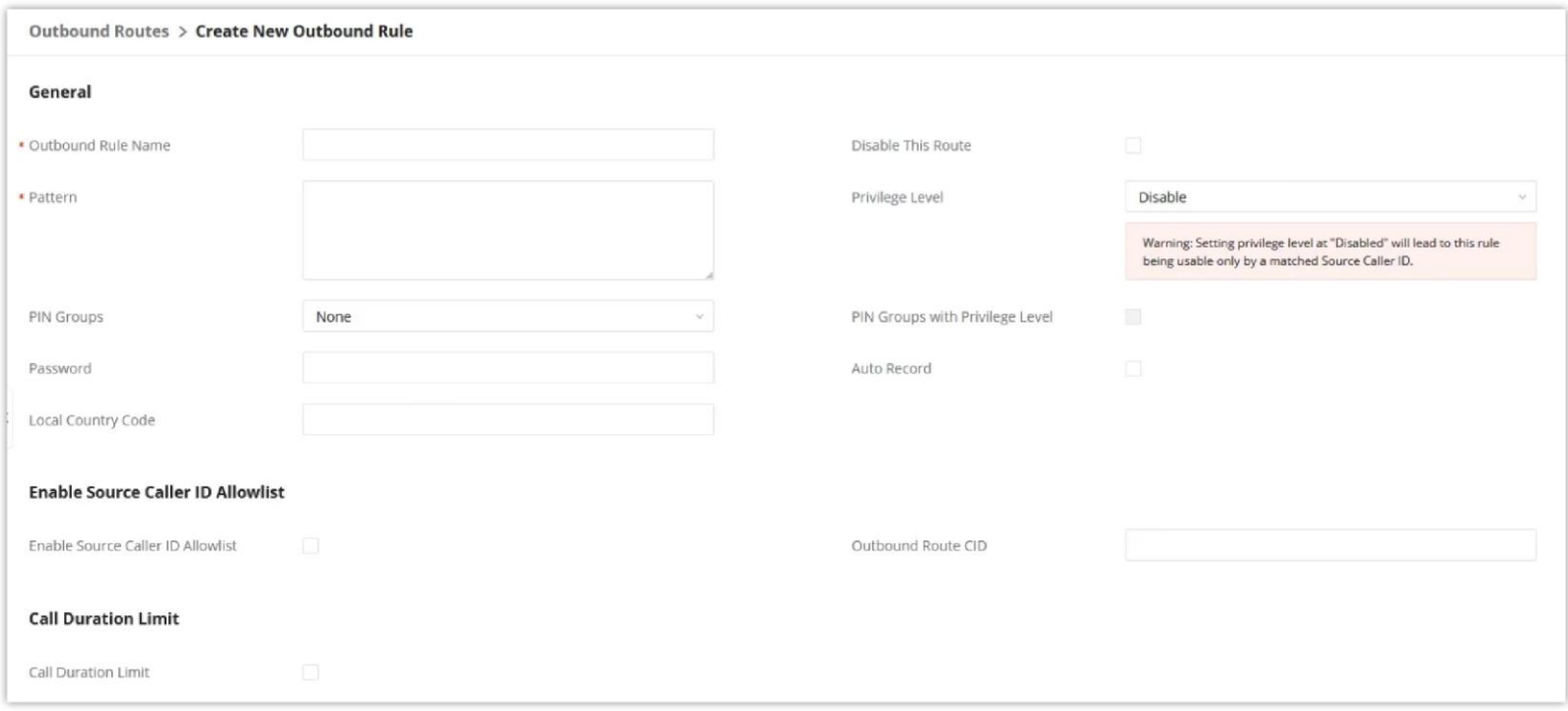
Trunk Security

A potential risk for trunks is unauthorized international and long-distance calls, which can result in unexpected high charges before the issue is noticed. Therefore, administrators must take special care when configuring trunks that would be charged for placing certain calls such as long-distance calls and international calls.

Outbound Rule Permissions

Users can apply one of four security measures on the UCM to control outbound calls.

1. Privilege Level
2. Enable Source Caller ID Whitelist
3. Password protection
4. PIN groups



Outbound Rule Permissions

Privilege Level

On the UCM, the supported 4 privilege levels are “Internal”, “Local”, “National” and “International” from the lowest to the highest. Outbound calls through trunk can be placed only if the permission level assigned to the caller is higher or equal to the privilege level of the outbound rule. Outbound call requests from users with privilege lower than the outbound rule will be rejected.

Source Caller ID Filter

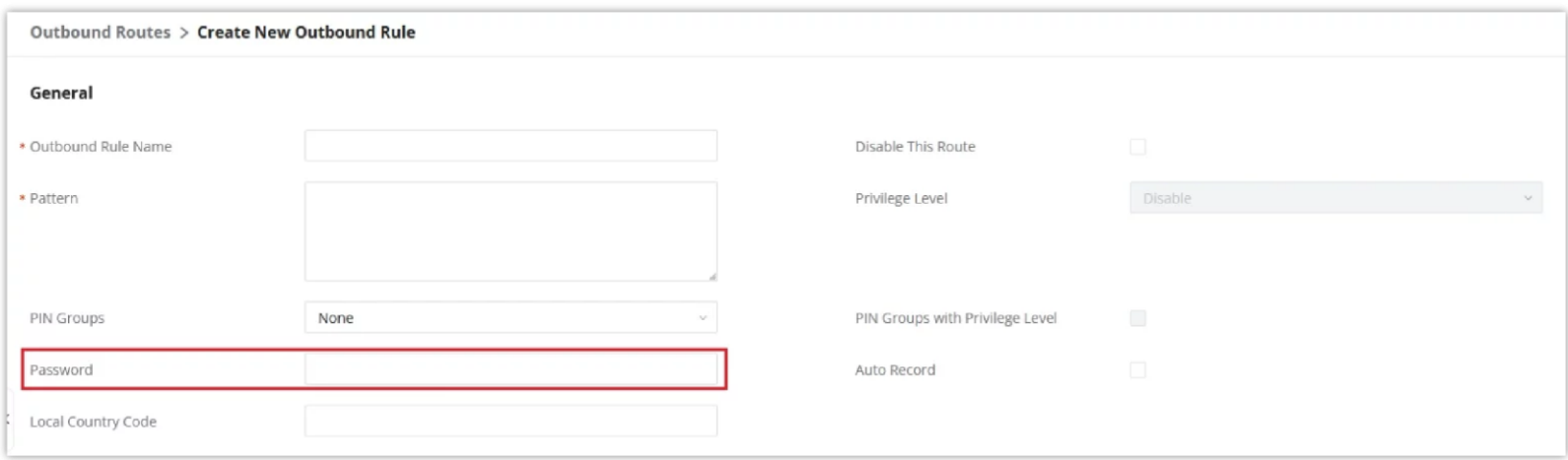
UCM administrators can specify the extensions/extension groups that can use the outbound rule. This can be done by selecting extension/extension groups or defining pattern for the source caller ID in “Source Caller ID pattern” field. The extension allowed to make outbound call will either need to be an extension in the selected list or match the defined pattern.

Source Caller ID Filter

For detailed configuration instructions, please refer to MANAGING OUTBOUND ROUTE section in white paper: How to manage inbound/outbound route on UCM6xxx

Password Protection

Administrators can protect outbound rules with passwords that would be requested by the UCM when callers try to use the configured routes.

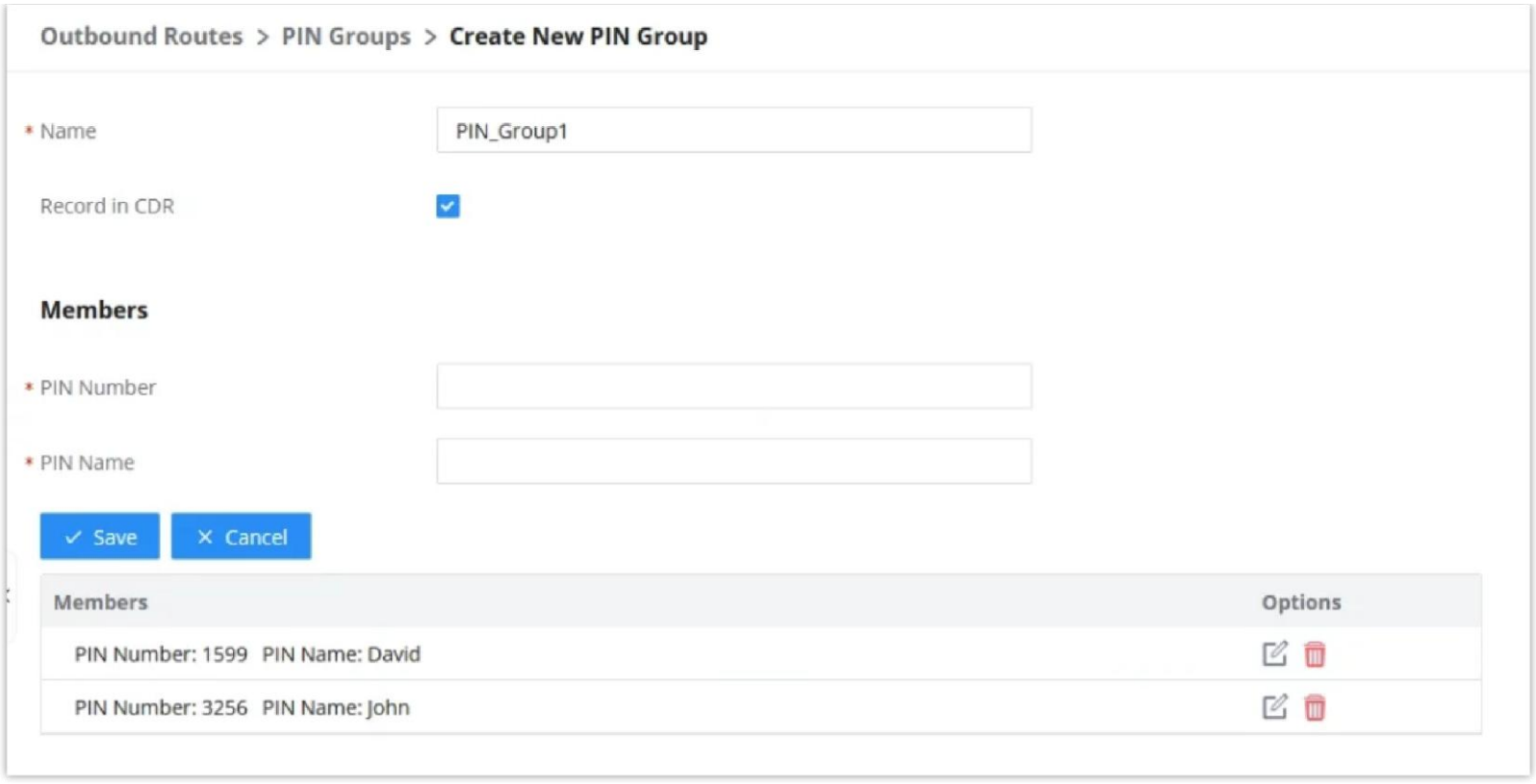


Password Protection

PIN Groups

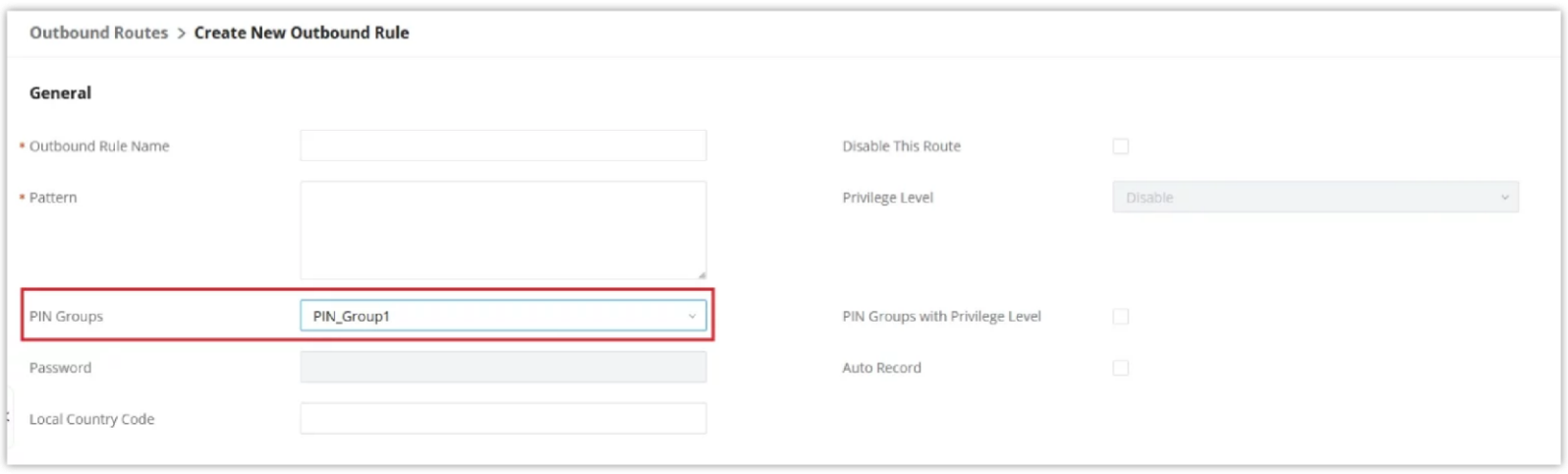
In the scenario where multiple users share the same phone, and the phone is used to make outbound calls, outbound routes can be set to require PIN entry to use. To set up a PIN group:

1. Navigate on to **Extension/Trunk→Outbound Routes→PIN Groups**
2. Click Add to create a new PIN group and enter the user names and passwords.



Adding PIN Groups

2. Save and apply. The PIN Group can now be selected in Outbound Routes. Each time one of the PIN Group members makes an outbound call, he/she will be requested to enter their PIN.

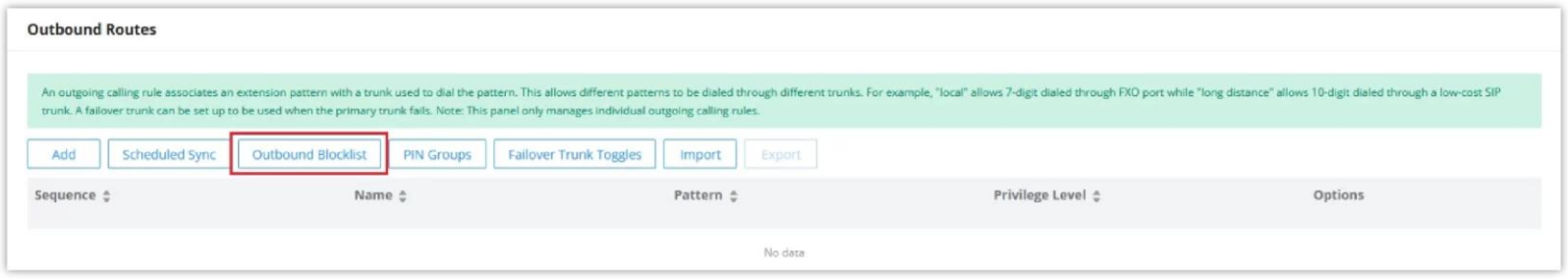


Outbound route with PIN group

Outbound Blacklist

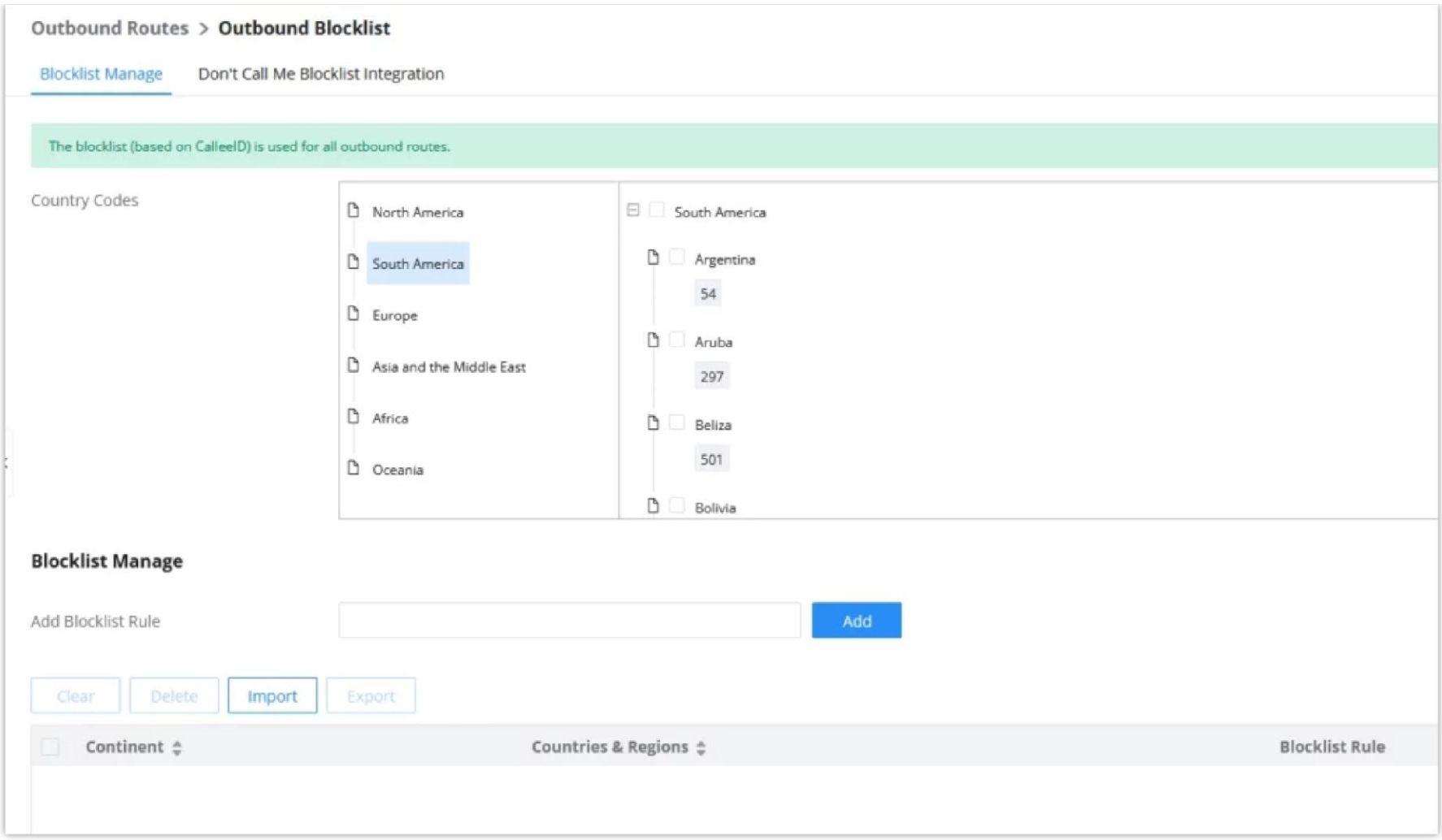
Managing Outbound Blocklist

Another way to secure your outbound routes is by setting a blacklist for the destinations that you do not want to allow to be dialed. It can be configured to prevent calls to certain countries which might result in additional financial charges. To set a blacklist for your outbound route, navigate to **Extension/Trunk →Outbound Routes**



Outbound Routes

Then select the countries that you want to include in the list of the countries that you don’t want the users to dial to.



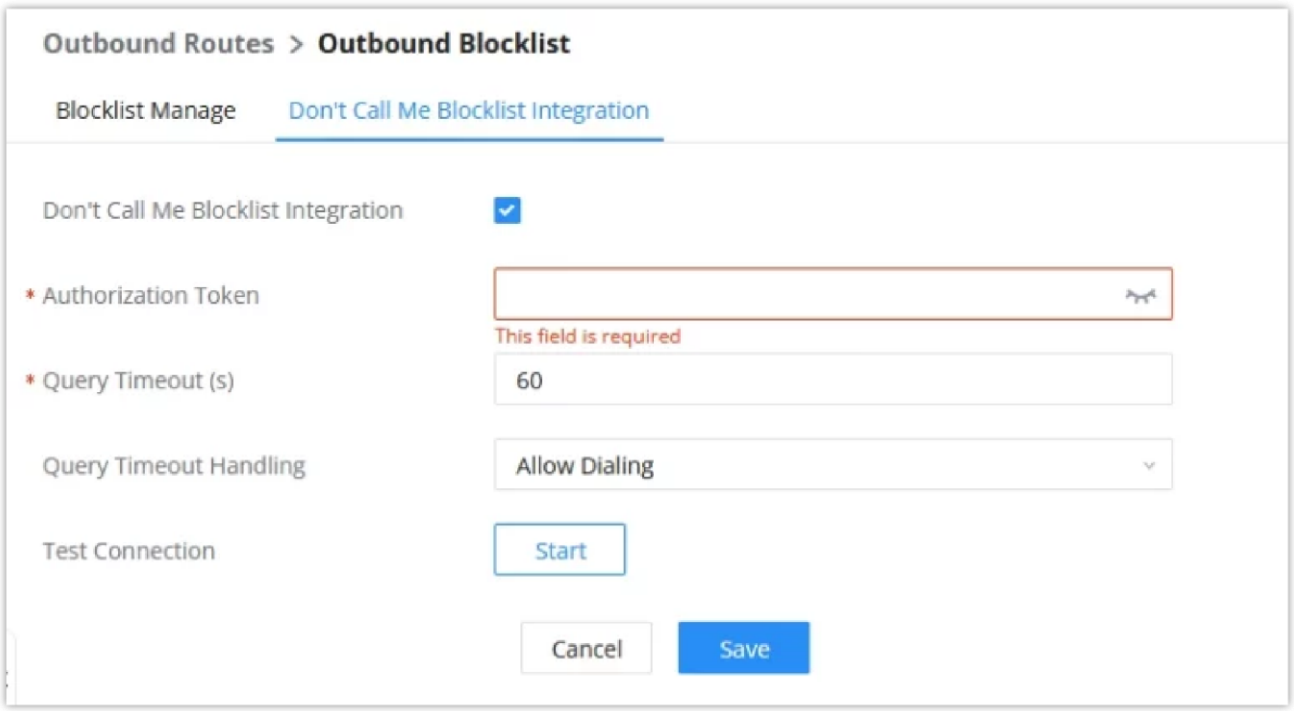
Managing Outbound Blocklist

You can also export the list to use on another UCM, or import one that you have already exported.

Don’t Call Me Blocklist Integration

The UCM63xx supports integration with a database containing blocked numbers to prevent unsolicited calls. During the dialing process, the UCM can query the blacklist API to verify if the dialed number is listed in the database. Based on the API response, the call will either be allowed or blocked accordingly.

Users can also decide whether to allow or block dialing if the configured Query Timeout (in seconds) elapses without a response.

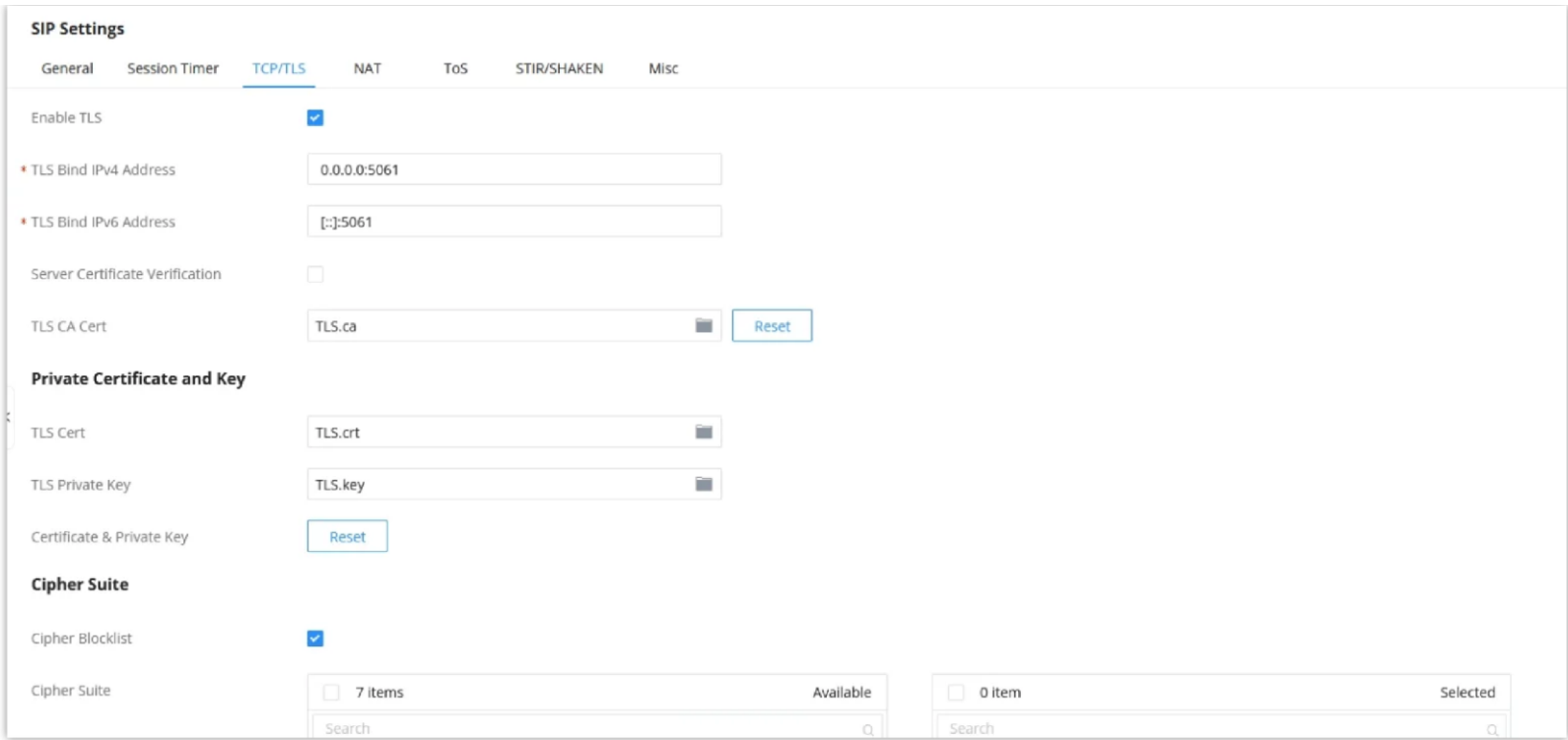


Dont Call Me Blocklist

TLS

UCM has the option to secure SIP packets with TLS encryption, allowing for safe transactions over untrusted networks and with authenticated parties.

TLS can be configured in **PBX Settings→SIP Settings→TCP/TLS**.



TLS Settings

1. Tick the "Enable TLS" box to activate TLS. (Enabled by default in the UCM63xx/A series).
2. Configure "Server Certificate Verification", "TLS CA Cert" and "TLS Cert" to achieve basic TLS authentication and encryption.
   - **TLS CA Cert**

Used when UCM is acting as the client to authenticate a server. If the server uses a self-signed certificate, that certificate should also be installed on the UCM for successful verification. If it is signed by a CA, then a copy of the CA server certificate should be installed.

   - **TLS Cert**

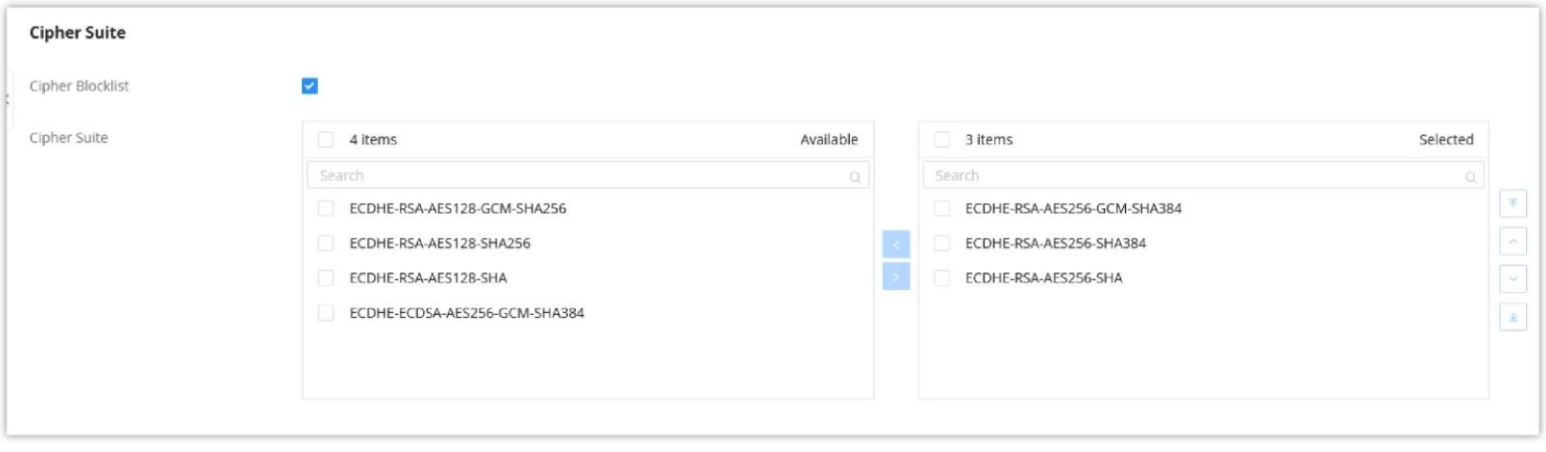
This process is used when UCM functions as the server. During the TLS handshake, the TLS certificate, which includes the server certificate and key, is sent to the client. The "common name" field in the server certificate should match the server host (either by IP address or domain name). This is required if the client is another UCM (not a standard, as some clients do not have this requirement for server authentication). If the common name does not match, authentication on the client side will fail, and the TLS connection will fail to establish.

   - **Server Certificate Verification**

Effective only when the UCM is acting as the client. If disabled, the certificate sent by the server will not be verified. This is useful for authentication between two peered UCMs using the factory certificate, which has "common name" configured with the value "localhost", which is not a valid host and will result in authentication failure. Skipping verification will not have any effect on the encryption itself. If enabled, the client will verify the server certificate with the "TLS CA Cert".

SIP endpoints will still need to be configured to use TLS in order to encrypt SIP messages sent to the UCM.

Users can also specify which SIP TLS encryption suites are supported on the UCM. By default all cipher are supported unless **Cipher Blocklist** is configured under **PBX Settings→SIP Settings→TCP/TLS**.



Firewall

The UCM firewall functionality consists of three components: Static Defense, Dynamic Defense, and Fail2ban. Each can be configured for specific types of malicious attacks.

Static Defense

Static Defense uses pre-configured filtering rules to protect the UCM. Three filtering rule types are supported: ACCEPT, REJECT, and DROP. These rules can be applied to service or specific source/destination IP addresses and ports. Static Defense can be configured in **System Settings→Security Settings→Static Defense**.

When creating or editing rules, the following options are available:

- Rule Name: A name to easily identify the rule and its purpose.
- Action: The action to perform for this rule. Accept, Reject, or Drop the connection if criteria is met.
- Type: The direction of the network traffic. IN for inbound traffic. OUT for outbound traffic.
- Interface: Select network interface where the traffic will go through (this option is only available for devices with both WAN and LAN ports).
- Service: The specific services to affect. FTP, SSH, Telnet, HTTP, and LDAP are available. Custom allows administrators to specify source/destination IP addresses and ports and the protocol.

Additionally, the following features are also available to further increase security:

1. Ping Defense

Protects against ping floods by not responding to ICMP echo requests.

2. SYN-Flood Defense

Protects against SYN floods by limiting the amount of SYN requests accepted per second.

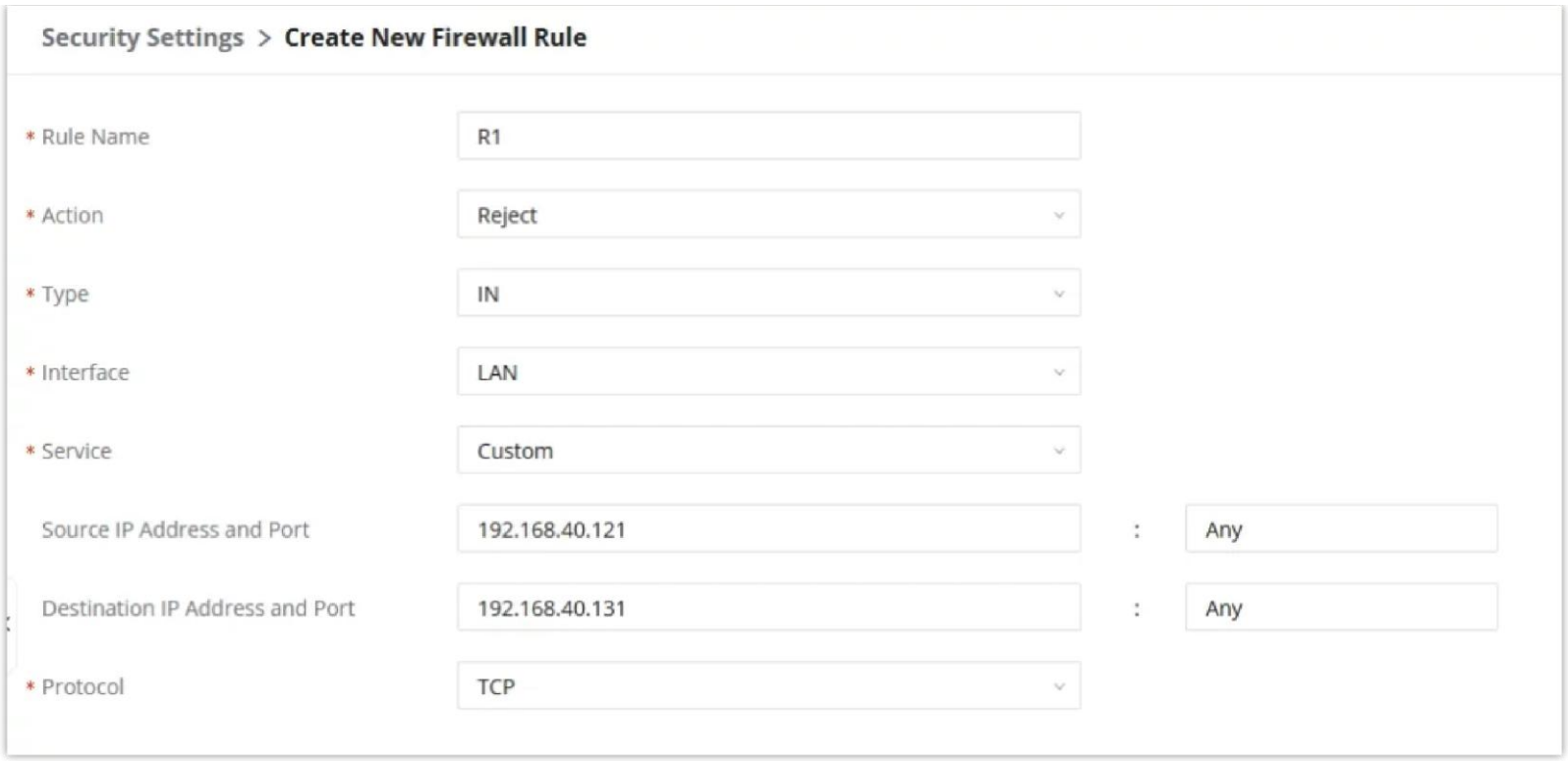
3. Ping-of-Death defense

Protects against ping packets larger than 64 KB.

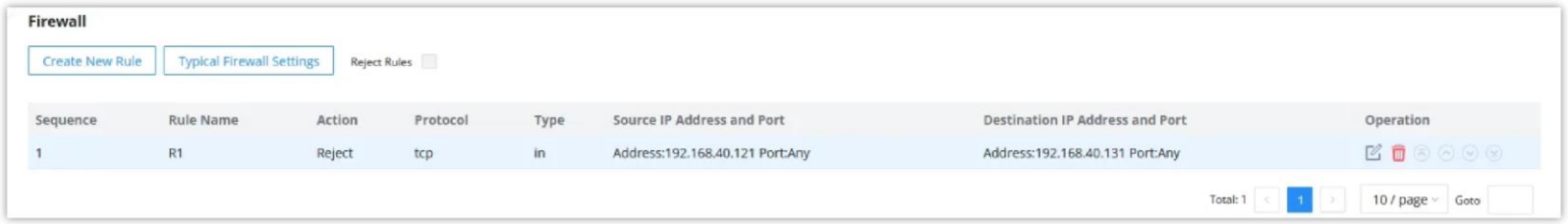
These settings can be enabled under **System Settings→Security Settings→Static Defense →"Typical Firewall Settings"**.

Static Defense Example: Blocking TCP Connection from a Specific Host

This example demonstrates how to set up a new rule to block a host with a specific IP address to connect to UCM using TCP connection. In the following figure, 192.168.40.121 is the host IP address and 192.168.40.131 is the UCM's IP address. Port 8089 on UCM is used for HTTP server/web UI access. This setting will block host on 192.168.40.131 to access UCM port 8089 using TCP connection.

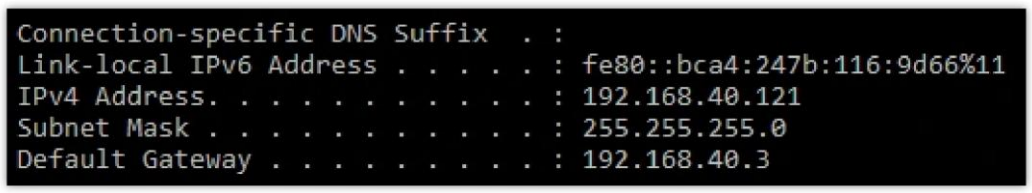


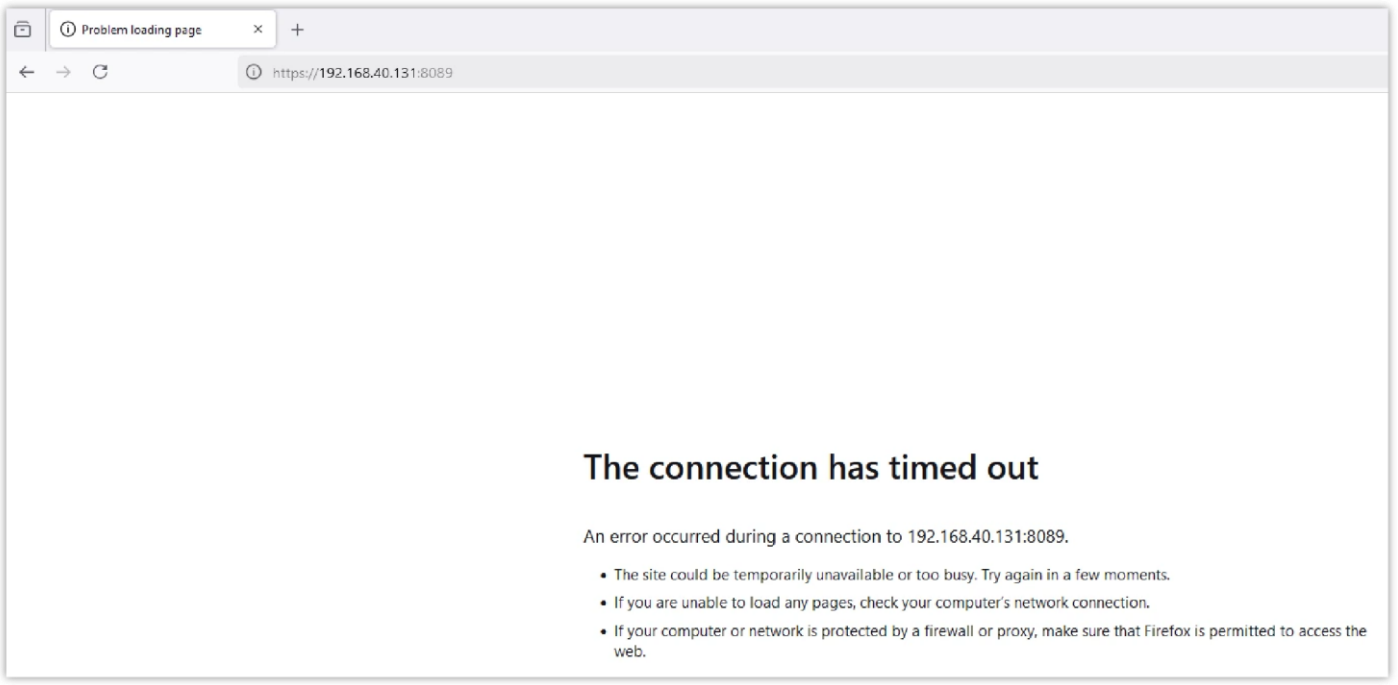
Firewall Rule Custom Configuration



Static Defense Blocking Host 19216840121 Using TCP Connection

After saving and applying the change, host 192.168.40.121 will not be able to access UCM web UI anymore.





Host blocked by UCM

Dynamic Defense

Dynamic Defense protects the UCM by blacklisting individual hosts that send excessive connection attempts or brute force attacks. On UCM6300/A, this requires **Network Settings> Basic Settings > Method** to be set to "Route". Dynamic Defense can be configured in **Security Settings > Dynamic Defense**, it will try to blacklist massive connection attempts or brute force attacks made by individual host.

Dynamic Defense's connection threshold and blacklist update interval can be adjusted in accordance to administrator preferences. Whitelist entries can be added to prevent specific IP addresses and ports from getting blocked.

For more configuration details, please refer to https://documentation.grandstream.com/knowledge-base/ucm630x-series-user-manual/

Geo-IP Access Control

Geo-IP Access Control allows administrators to restrict access to the UCM based on the source country or geographic region of an inbound connection. When enabled, the UCM evaluates the originating IP address against a geographic database and blocks connections originating from countries that are configured as restricted.

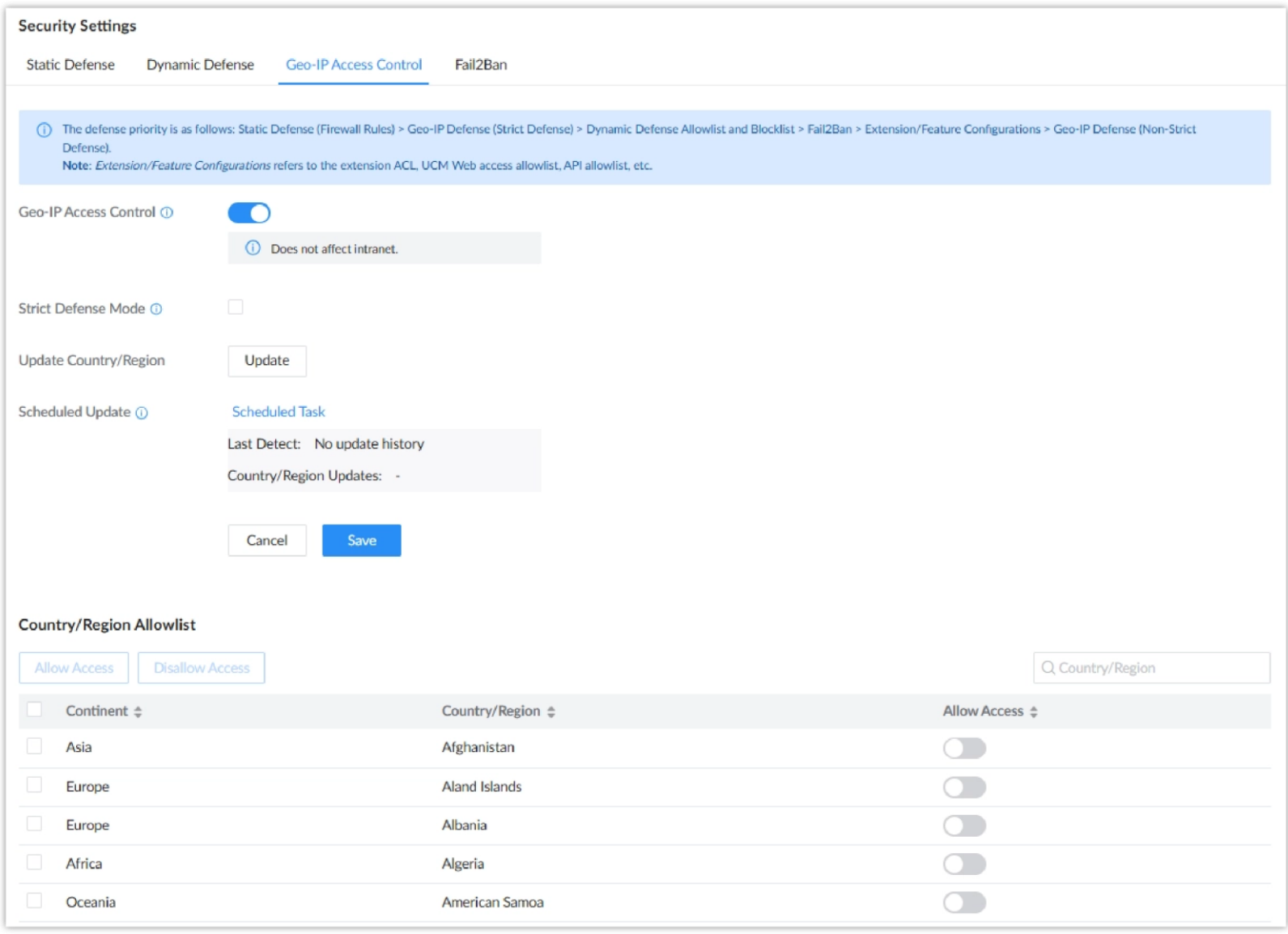
This restriction is applied system-wide and affects the following services:

- **Web UI access (administrator and user portals)**
- **API requests**
- **Extension registration**

Administrators can manage the list of blocked countries manually or configure automatic database refresh at scheduled intervals to maintain accuracy as public IP assignments change.

To configure Geo-IP Access Control, please refer to the following instructions:

1. Navigate to **System Settings > Security Settings > Geo-IP Access Control**.
2. Enable Geo-IP Access Control.
3. Enabling "*Strict Defense Mode*" will result in the UCM dropping all the data packets received from disallowed countries and regions. Access request (including normal calls) will be denied to ensure system security.
   Note: This option will override any configuration set in other allow lists (e.g., API Allowlist, Extension ACL, Web Access Allowlist, etc...). When enabling this configuration for the first time, the UCM will prompt the user to reload the web server, this will log the user out of the session.
4. Select one or more countries or regions using the checkboxes.
5. Click the *"Allow Access"* button to permit traffic from those locations, or *"Disallow Access"* to remove permission. Or use the per-country toggle in the *Allow Access* column to quickly enable or disable access for individual entries.
6. (Optional) Click *Update* to refresh the Geo-IP database if required, or configure *Scheduled Update* to automatically keep the database current.
7. Apply the configuration.



Geo IP Access Control Settings

Important Note:

If the UCM detects that your current management IP belongs to a blocked country, a warning banner will appear recommending that you allow access for that country before saving changes. Always verify that your own administrative network is not blocked to avoid losing access.

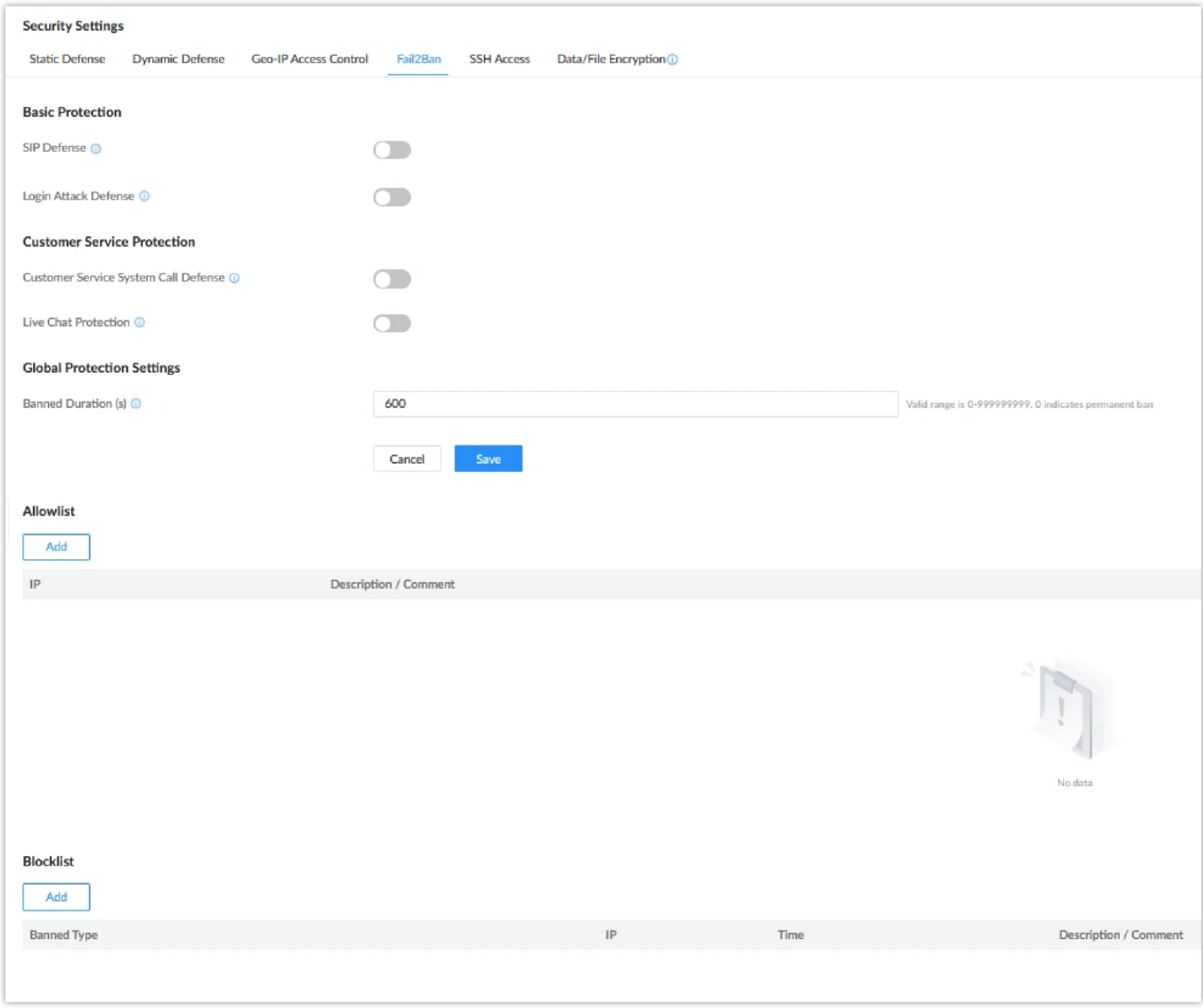
Note

Any configured IP addresses in other allowlists will be permitted to access regardless of the configuration of the Geo-IP Access Control.

Fail2ban

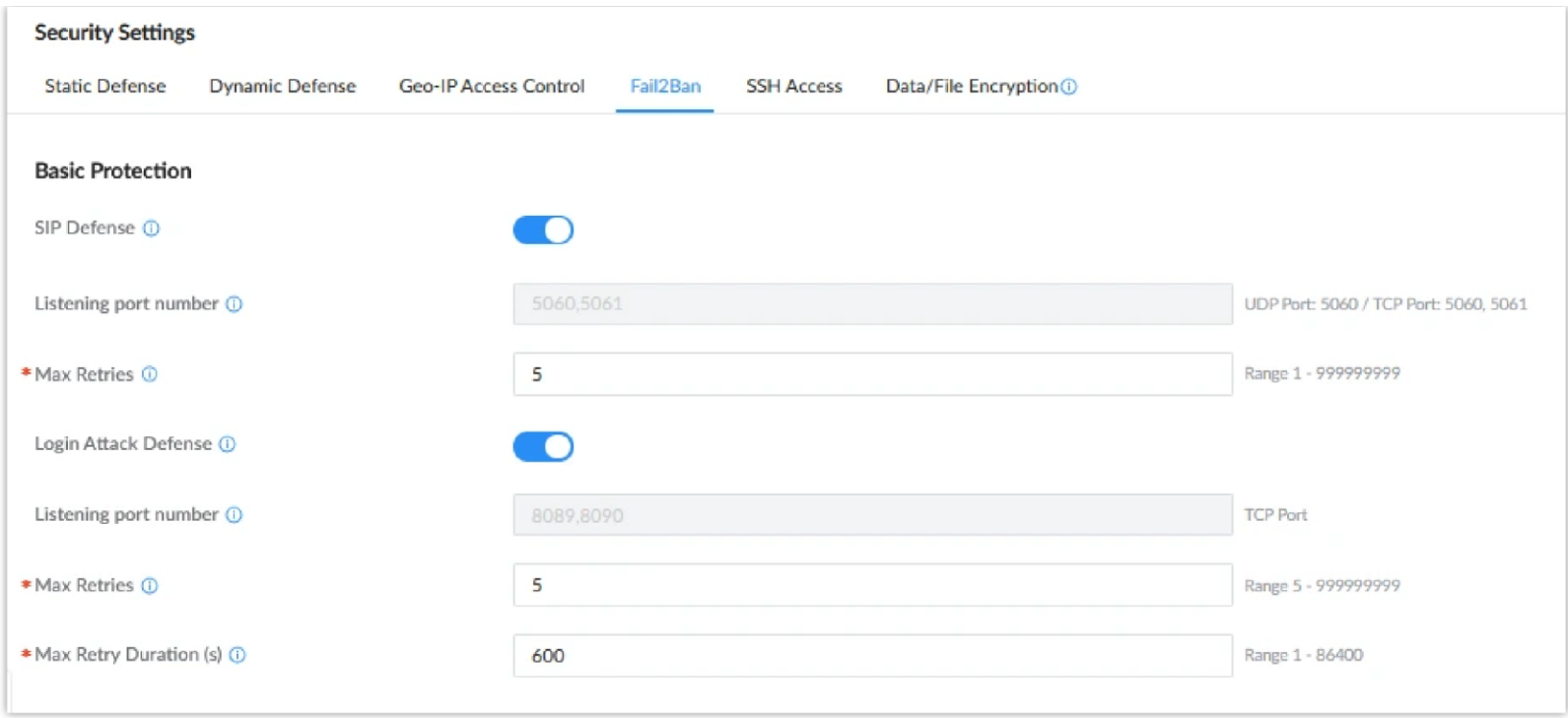
Fail2ban protects the UCM by detecting excessive failed login attempts and SIP requests and blocking any further attempts from the same host.

Fail2Ban can be configured in **System Settings > Security Settings > Fail2Ban**. By default, Fail2Ban is enabled.

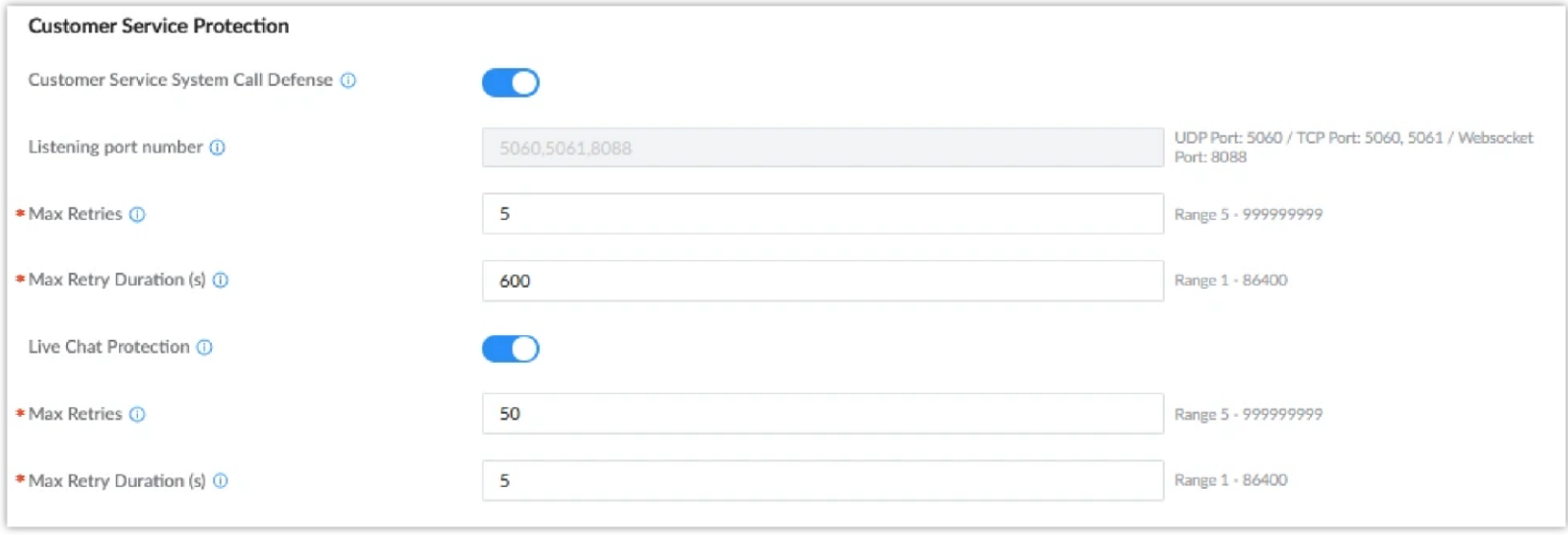


Fail2Ban Settings

- **Banned Duration (s):** The amount of time in seconds that a host is banned for. A value of "0" means an permanent ban. Set to 600 seconds by default.
- **Allowlist:** The set of hosts that are exempt from Fail2ban actions. IPs in this list will not be banned, even if they exceed the configured threshold for failed SIP registrations or login attempts. You can manually add trusted hosts to this list.
- **Blocklist:** The set of IP addresses currently banned by the UCM, including the ban type and remaining duration. You can also manually add IP addresses to this list to block them immediately.



SIP Defense Login Attack Defense



Customer Service System Call Defense Live Chat Protection

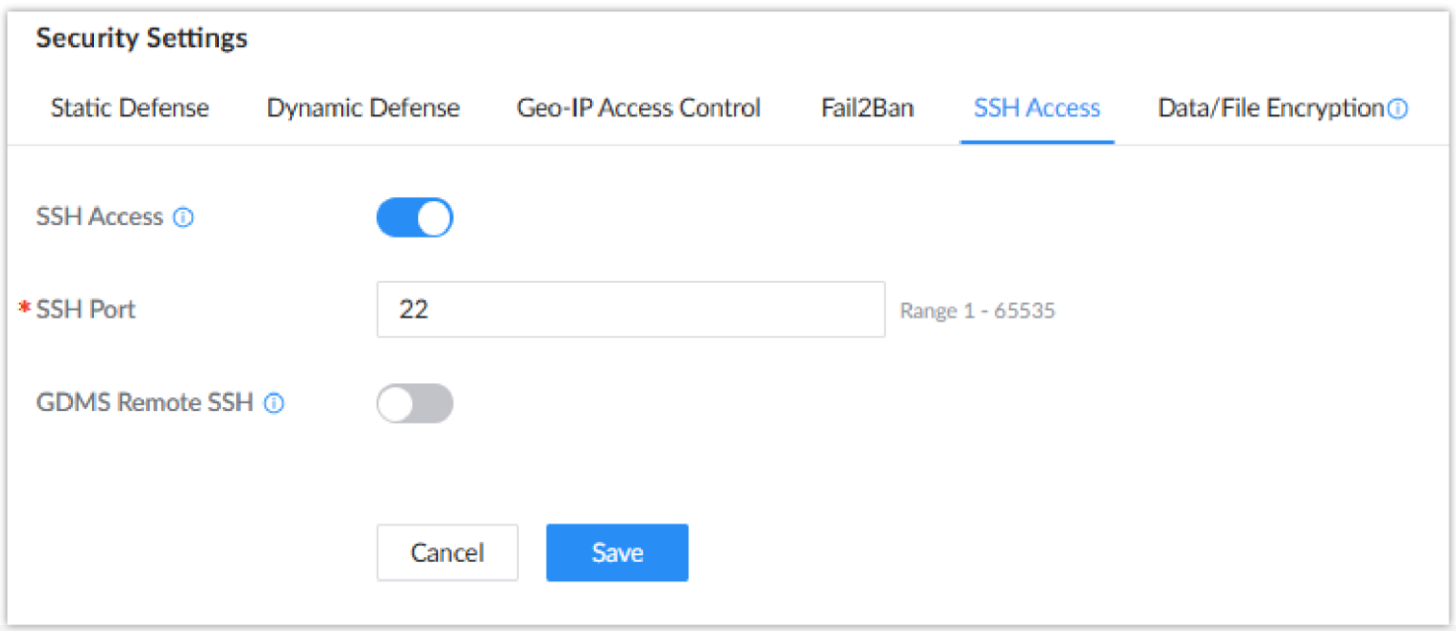
- **SIP Defense:** Protects against excessive failed SIP REGISTER, INVITE, and SUBSCRIBE requests. If the retry limit has been reached, the UCM will not respond to any more SIP requests from the same host. The Listening port number value will match the configured SIP port number in the **PBX Settings→SIP Settings**.

- **Login Attack Defense:** Protects against excessive failed login attempts. If the retry limit has been reached, the UCM will prevent the host from accessing the UCM web UI. The Listening port value will match the configured port number in **System Settings→HTTP Server→Port**.

- **Customer Service System Call Defense:** Enable call defense in the customer service system. It Protects against excessive call generation when Click2Call feature is enabled. If the retry limit has been reached, the UCM will not respond to any more SIP requests from the same host.
- **Live Chat Protection:** Blocks excessive chat attempts. Once the number of chat attempts from an IP address has reached the *Max Retries* value configured for this defense, the IP address will banned for the amount of time configured in the *Banned Duration* field.

SSH Access

Users can enable or disable SSH access by accessing **System Settings** > **Security Settings > SSH Access.**

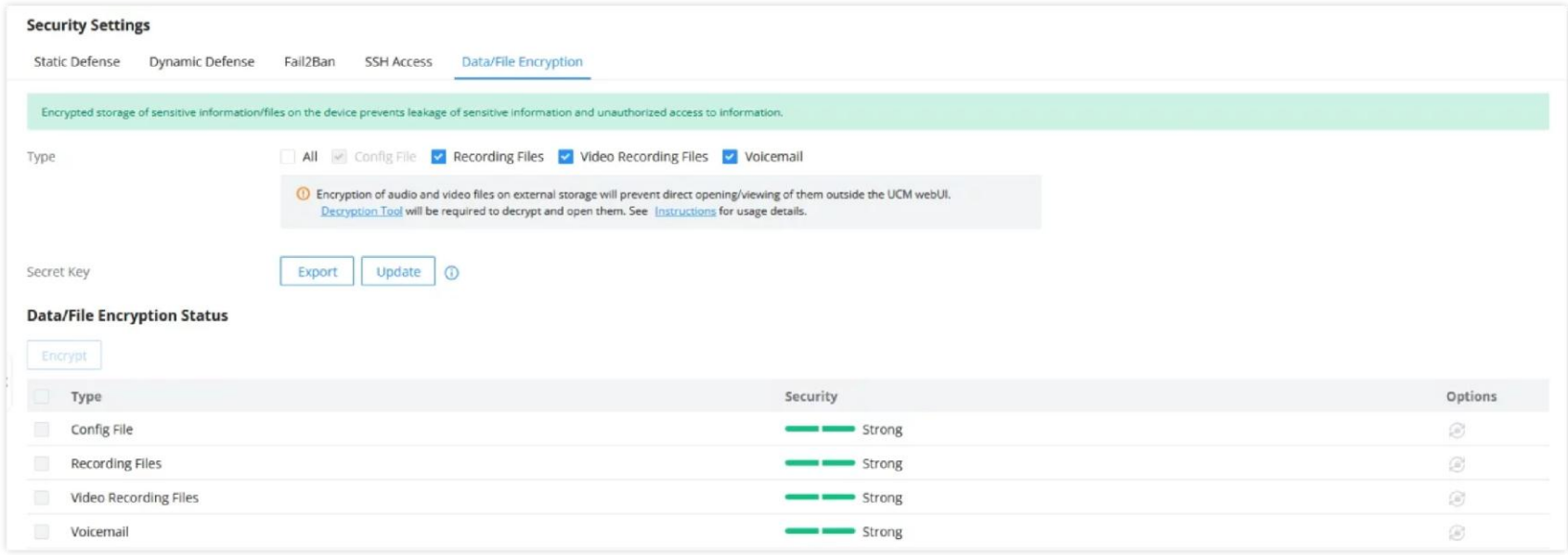


SSH Access Settings

- **SSH Access:** This option allows SSH access for system debugging, using the "admin" username and the super administrator's password. It is disabled by default for security reasons and should only be enabled if needed.
- **SSH Port:** Configure the port to use for SSH service.
- **GDMS Remote SSH:** If enabled, the system will allow remote SSH access via the GDMS platform. This option is turned off by default, and it is strongly recommended to turn off this option when remote troubleshooting is not required.

Data/File Encryption

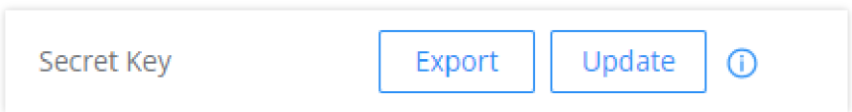
The UCM6300 Series offers encryption for data stored on the internal storage space of the UCM or on the attached storage units (e.g., SD Card, USB HDD/SSD, USB Flash Drive). To access this feature, please navigate to **PBX Settings** > **Security Settings** > **Data/File Encryption**.



DataFile Encryption

Once the user chooses which data to encrypt, any data created after this configuration will be encrypted, however, all the data which has been created prior to this configuration is not encrypted.

When the user click on "Export" button, a CSV file which contains the secret key will be downloaded. This key can be stored safely and used to decrypt the data later on.



Secret Key ExportUpdate

The secret key can be updated using the "Update" button, this would require entering the administrator's password to allow the user to change the secret key.

To open and play encrypted audio/video files outside of the UCM system, users need a decryption tool (found on the Grandstream Tools page), a key file and the password for it (set when exporting the key file).

For more information on how to use the decryption tool, please refer to the following guide :

UCM6300/A Series IP PBX – CDR Tool Guide

AMI

Asterisk Manager Interface (AMI) is supported on UCM with restricted access. Please refer to the following link for detailed documentation on the feature:

https://documentation.grandstream.com/knowledge-base/ami-asterisk-management-interface/

It is highly recommended not to enable AMI on a UCM that is placed on a public or untrusted network unless precautions have been taken to prevent unauthorized access and restrict permissions. AMI access allows users to originate calls and view sensitive information on the UCM.

* ***Asterisk is a Registered Trademark of Digium, Inc.***