GRANDSTREAM
CONNECTING THE WORLD

Grandstream Networks, Inc.

UCM series IP PBX

Security Manual

Table of Contents

Table of Figures

OVERVIEW

This document presents a summary of security concerns on UCM. It covers the security risks and related configurations that users need to consider when deploying the UCM.

The following sections are covered in this document:

- **Web UI access**
  Web UI is secured by user login and login timeout mechanism. Two-level user management is configurable. Admin with limited access can be created by the default super administrator.

- **Extension security**
  This includes SIP/IAX password for authentication, IP access control and SRTP.

- **Trunk security**
  Trunk security is achieved mainly by setting the privilege level, configuring source caller ID filter to filter out outbound call requests from unwanted source

- **TLS**
  This is to secure the SIP signaling.

- **Firewall mechanism**
  Three types of firewall mechanism can be configured to protect UCM against malicious attacks: Static Defense, Dynamic Defense (UCM6510 and UCM6102/UCM6202/UCM6204/UCM6208 only) and Fail2ban.

- **AMI**
  Using AMI feature comes with security concerns for UCM administrators to consider.

This document is subject to change without notice. The latest electronic version of this document is available for download here:
http://www.grandstream.com/support

WEB UI ACCESS

UCM HTTP Server Access

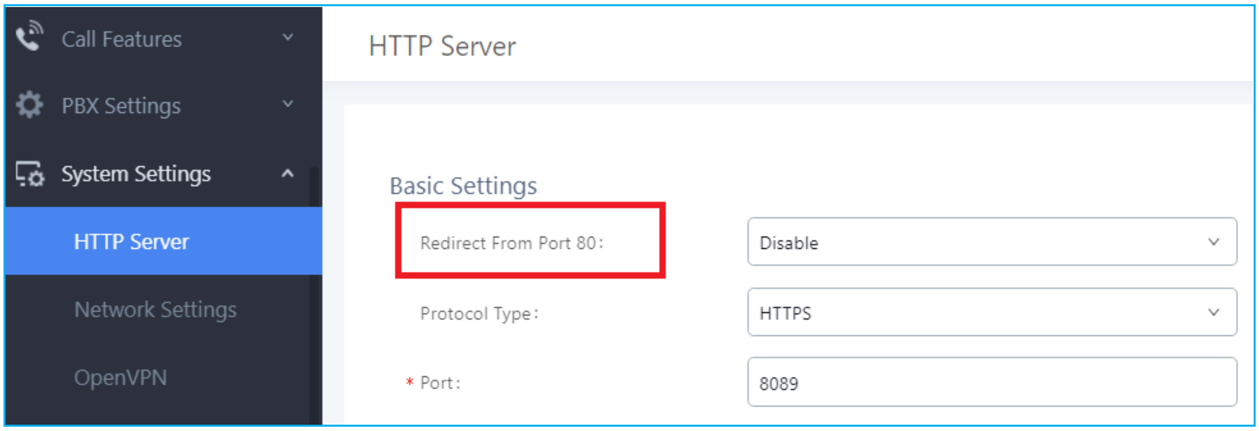
The UCM embedded web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a web browser such as Microsoft IE, Mozilla Firefox, Google Chrome and etc. This is the most important tool to configure all the settings on the UCM. It's also the immediate interface for the administrator to access configurations, user status and all the system information. Therefore, it's crucial to understand that directly placing the UCM on public network could expose the domain name / IP address of the UCM and pose serious security concerns.

Protocol Type

HTTP and HTTPS web access are supported to access the UCM web UI. It can be configured under web UI→Settings→HTTP Server. The protocol type is also the protocol used for zero config when the endpoint device downloads the config file from the UCM. Therefore, it's recommended to use HTTPS instead of HTTP to secure the transactions and prevent unauthorized access.

Note also that by default we are using HTTP/HTTPS ports that are different from the well know ports 80 and 443.

It is recommended to disable the option "Redirect From Port 80".



HTTP Server

Basic Settings

Redirect From Port 80: Disable

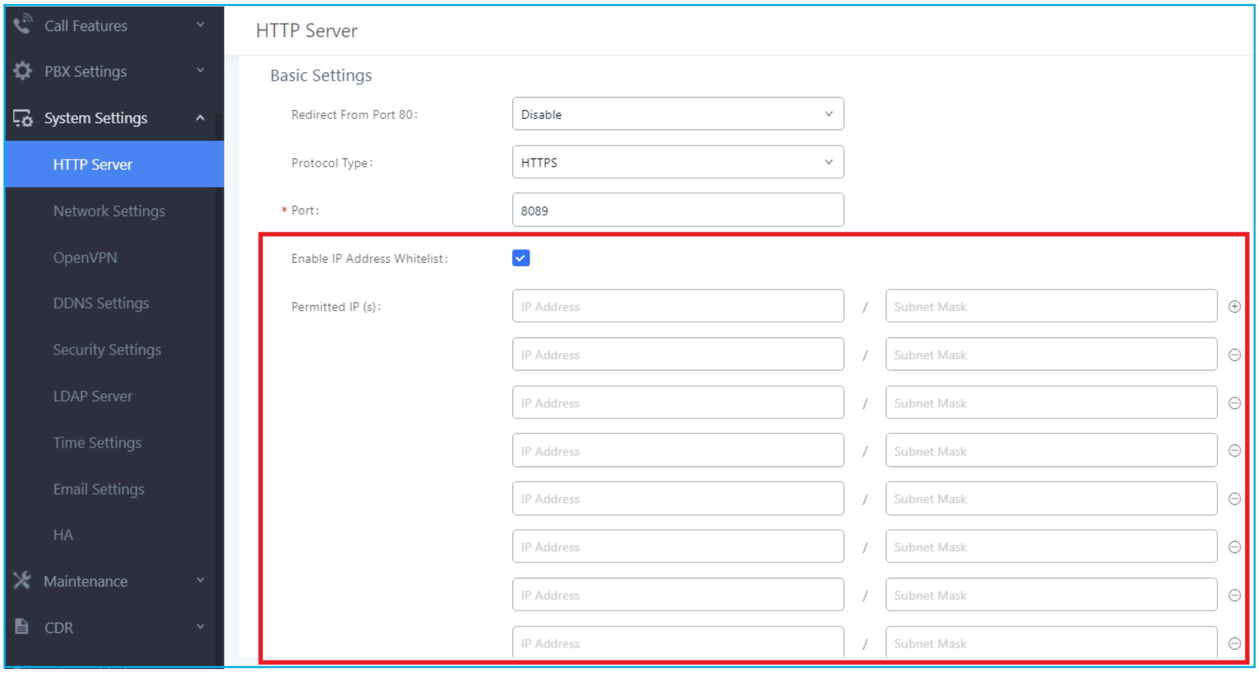
Protocol Type: HTTPS

* Port: 8089

Finally, users have the option to specify a list of UP to 10 IP addresses which will be allowed to access the UCM web GUI, otherwise the connection will be refused for any IP address not figuring in the white list.

To add IPs to the whitelist, go under menu web UI→Settings→HTTP Server:

- Enable the option "Enable IP Address Whitelist"
- Enter the permitted IP(s) by specifying both the address and the Subnet mask.



HTTP Server

Basic Settings

Redirect From Port 80: Disable

Protocol Type: HTTPS

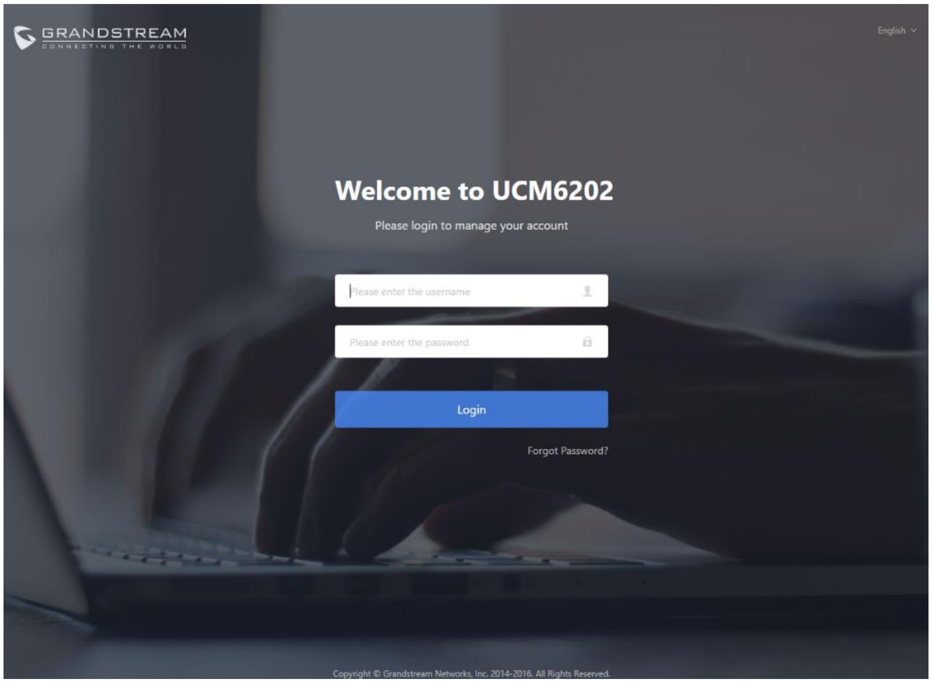
* Port: 8089

Enable IP Address Whitelist: ☑

Permitted IP (s): IP Address / Subnet Mask

User Login

UCM web UI access is restricted by user login. Username and password are required when logging in to web UI.



Welcome to UCM6202

Please login to manage your account

Copyright © Grandstream Networks, Inc. 2014-2016. All Rights Reserved.

Figure 1: UCM6202 Web UI Login

The factory default value of "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. Older units and UCM6100 series have default password “admin”.

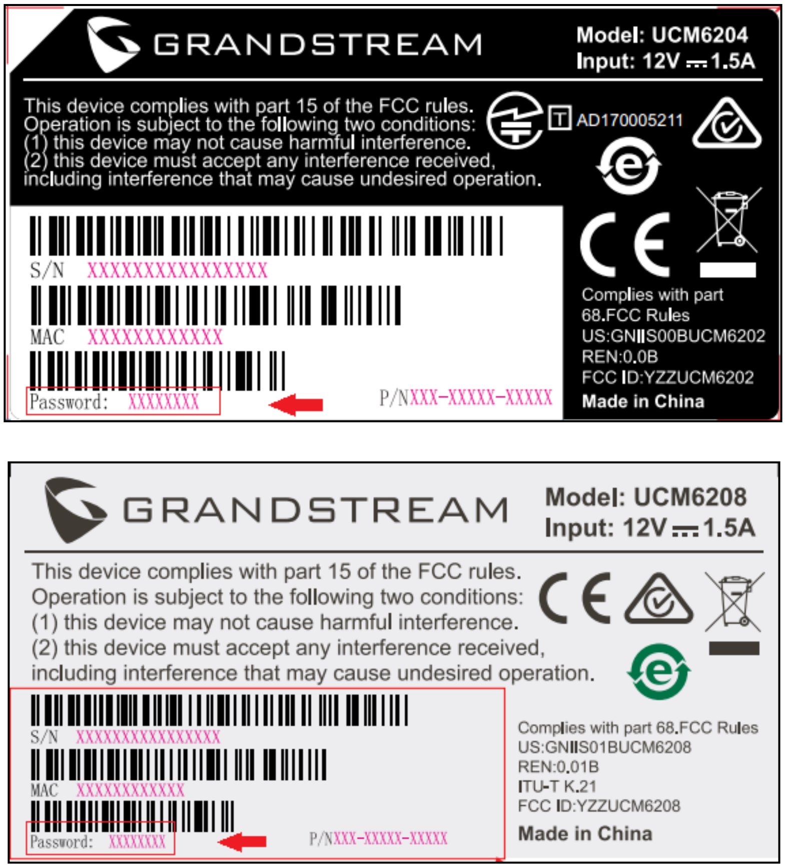

GRANDSTREAM
Model: UCM6204
Input: 12V ⎓ 1.5A
This device complies with part 15 of the FCC rules.
Operation is subject to the following two conditions:
(1) this device may not cause harmful interference.
(2) this device must accept any interference received, including interference that may cause undesired operation.
AD170005211
S/N XXXXXXXXXXXXXXXX
MAC XXXXXXXXXXXX
Password: XXXXXXXX
P/NXXX-XXXXX-XXXXX
Complies with part 68.FCC Rules
US:GNIIS00BUCM6202
REN:0.0B
FCC ID:YZZUCM6202
Made in China
GRANDSTREAM
Model: UCM6208
Input: 12V ⎓ 1.5A
This device complies with part 15 of the FCC rules.
Operation is subject to the following two conditions:
(1) this device may not cause harmful interference.
(2) this device must accept any interference received, including interference that may cause undesired operation.
S/N XXXXXXXXXXXXXXXX
MAC XXXXXXXXXXXX
Password: XXXXXXXX
P/NXXX-XXXXX-XXXXX
Complies with part 68.FCC Rules
US:GNIIS01BUCM6208
REN:0.01B
ITU-T K.21
FCC ID:YZZUCM6208
Made in China

Figure 2: Default Random Password

It is highly recommended to change the default password after login for the first time.

To change the password for the default user “admin”, go to web GUI→Settings→Change Password page. The new password has to be at least 4 characters. The maximum length of the password is 30 characters. The minimum requirement for the login password is as below if “Enable Strong Password” (on web GUI→ PBX→Internal Options→General) is turned on:

- Must contain numeric digit.
- Must contain at least one lowercase alphabet, uppercase alphabet or special character.

Strong password with a combination of numbers, lowercase alphabet characters, uppercase characters and special characters is always recommended to protect your login.

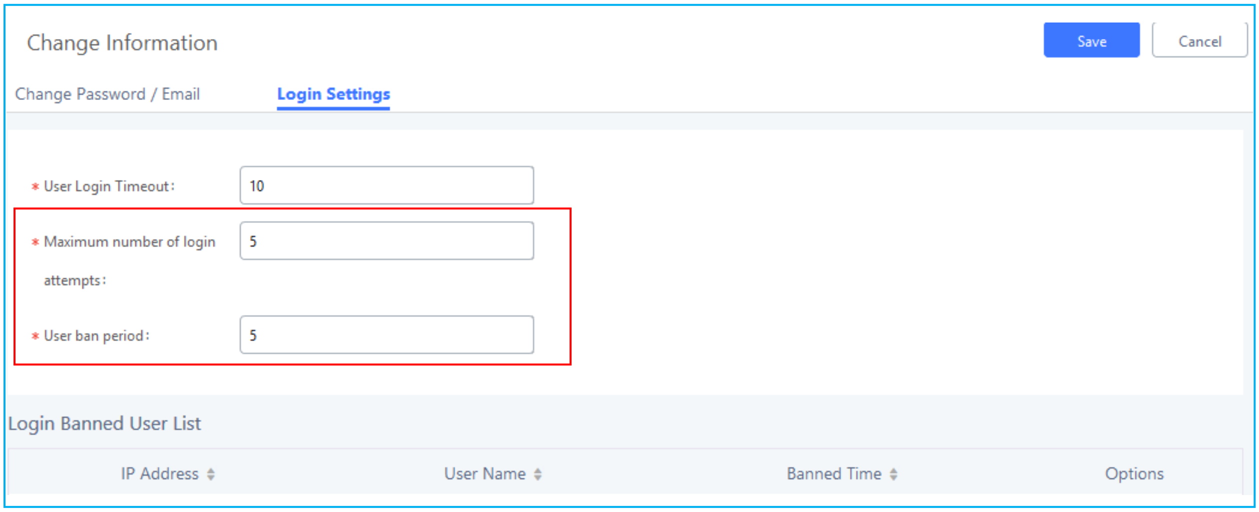
Login Settings

An authenticated user of the UCM web UI may log in the system and then leave the active session on a terminal unattended without intentionally logging-off from the system. An adversary with access to the terminal could then have access to the UCM, meaning all the configuration and status information could be exposed and changed intentionally or unintentionally.

UCM provides protection from such vulnerability using login timeout. After the user logs in the UCM web UI, the user will be automatically logged out after certain timeout. This timeout value can be specified under UCM web GUI→Maintenance→Change Information→Login Settings page. In the case that the user doesn't make any operation on web GUI within the timeout period, the user will be logged out automatically and the web UI will be redirected to the login page, requiring password to access the web pages.

If the login timeout period is set to a short enough time, the chances of an adversary gaining access to an unattended terminal are significantly reduced. However, the timeout period cannot be too short that an authenticated user becomes annoyed by frequent automatic logouts during normal use. Therefore, users shall set it to a value according to actual usage and situation. The default value of login timeout is 10 minutes.

Along with the login timeout feature, the UCM supports also user banning upon unsuccessful login attempts with the possibility to configure the maximum number of allowed failed login attempts as well as settings the ban period as shown on the below figure.



* User Login Timeout: 10

* Maximum number of login attempts: 5

* User ban period: 5

Login Banned User List

IP Address	User Name	Banned Time	Options

Figure 3: Login Settings

User Management Levels

On UCM, Four privilege levels for web UI users are supported:

- **Super Admin**: high priority.
- **Admin**: low priority.
- **Custom level**: custom priority.
- **Consumer**: Low Priority

Super administrator can access all pages on UCM web UI, change configuration for all options and execute all the operations, while normal administrator created by super administrator has limited access. Normal administrator can access all pages on UCM web UI except the following:

- Maintenance→Upgrade
- Maintenance→Backup
- Maintenance→Cleaner
- Maintenance→Reset/Reboot
- Settings→User Management→Operation Log

A "Super Admin" user with username "admin" is innately configured in the UCM at the factory setting. 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", "Custom" and "Consumer".

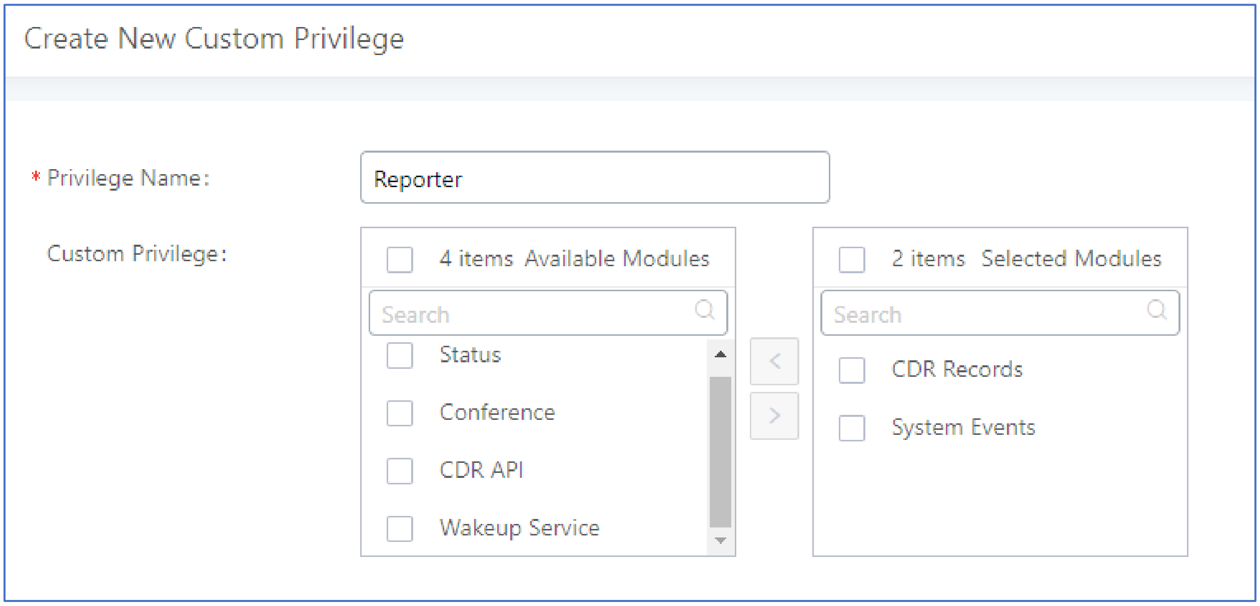
Super Admin also has the authority to view operations done by all the users in web GUI→Maintenance→Operation Log where normal users with lower privilege level "Admin" don't have access.

If there are more than one PBX administrator required to manage the UCM in your enterprise, it's highly recommended for the super administrator to create lower privilege administrators in order to manage the UCM together, instead of handing out super administrator password to all the other users who may need access the UCM web UI. The super administrator can also monitor the operation log to keep a record as well as ensure no abnormal operations done on the PBX.

While In case the super admin wants to assign some users specific privileges, the custom privilege user level can be helpful by giving him access to one or more of the following items:

- View Status Information
- Manage Conferences
- System Events
- CDR Reports
- CDR API
- Wakeup Service

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


Create New Custom Privilege

* Privilege Name: Reporter

Custom Privilege:

□ 4 items Available Modules
Search
□ Status
□ Conference
□ CDR API
□ Wakeup Service

□ 2 items Selected Modules
Search
□ CDR Records
□ System Events

Figure 4: Creating Custom Privilege Levels

From the security perspective, this feature can be helpful by giving each person the level of access that they just need, no more nor less.

The last user access level is the "Consumer" level, this is the default assigned one for user portal access where each user can access the UCM portal using his/her extension number and password in order to manage their own data and benefit from the value-added feature. This way normal users don't have access to configuration modules/items than can affect the whole system and cannot access to advanced maintenance operations.

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” (on web GUI→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.

If “Enable Strong Password” (on web GUI→ **PBX Settings→General Settings**) is enabled, the password must be alphanumeric which should contain numeric digit and at least one lower case alphabet or upper-case alphabet, or special character.

It is recommended to use random password and strong password to reduce the chance that the password being guessed or cracked out.

Strategy of IP Access Control

The UCM administrator could control what IP address(s) is allowed to register to a certain extension by editing “strategy” option under extension configuration dialog→“Media” tag. Make sure to configure the “strategy” option to the smallest set to block registration attempts from anyone that doesn’t need to register to the account.

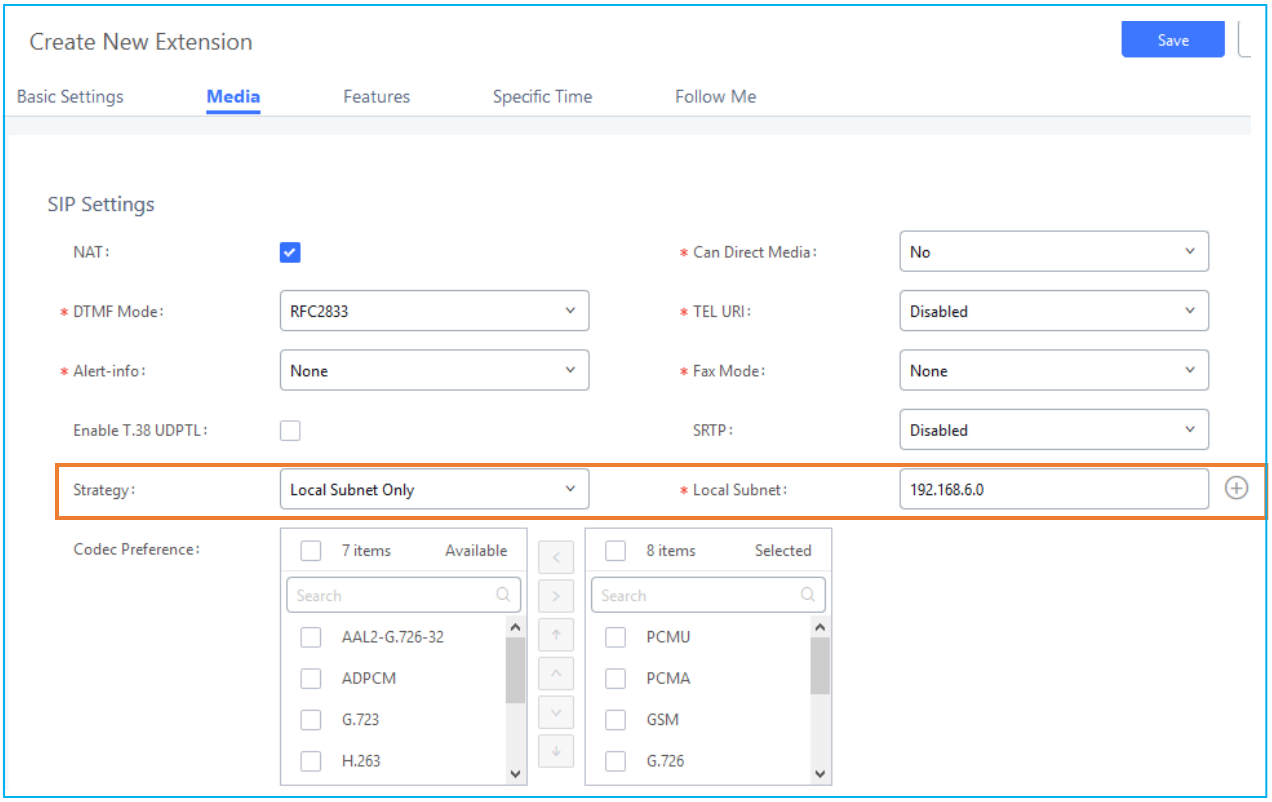
The strategy options are:

- “Local Subnet Only”: allows register requests from local IPs only. By default, the local subnet where the UCM is location is allowed. User could also add more local subnets where devices are allowed to register to this extension.
- “A Specific IP Address”: allows register requests from one user specified IP only.
- “Allow All”: the registration address is the entire Internet which is least recommended.

Example: Local Subnet Only

1. Assuming there are multiple subnets within the office and the devices in all subnets can reach each other. The network administrator would like to allow only devices in 192.168.40.x network to register to this UCM.

2. Under UCM web UI extension dialog, configure “Local Subnet Only” for “Strategy” option and 192.168.40.0 for “Local Subnet”.


Create New Extension

SIP Settings

NAT: ☑

* Can Direct Media: No

* DTMF Mode: RFC2833

* TEL URI: Disabled

* Alert-info: None

* Fax Mode: None

Enable T.38 UDPTL: □

SRTP: Disabled

Strategy: Local Subnet Only

* Local Subnet: 192.168.6.0

Codec Preference:

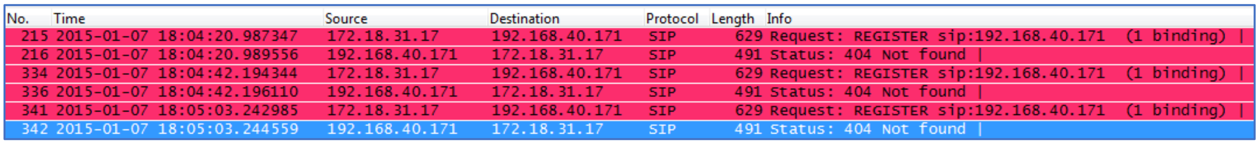
□ 7 items Available
Search
□ AAL2-G.726-32
□ ADPCM
□ G.723
□ H.263

□ 8 items Selected
Search
□ PCMU
□ PCMA
□ GSM
□ G.726

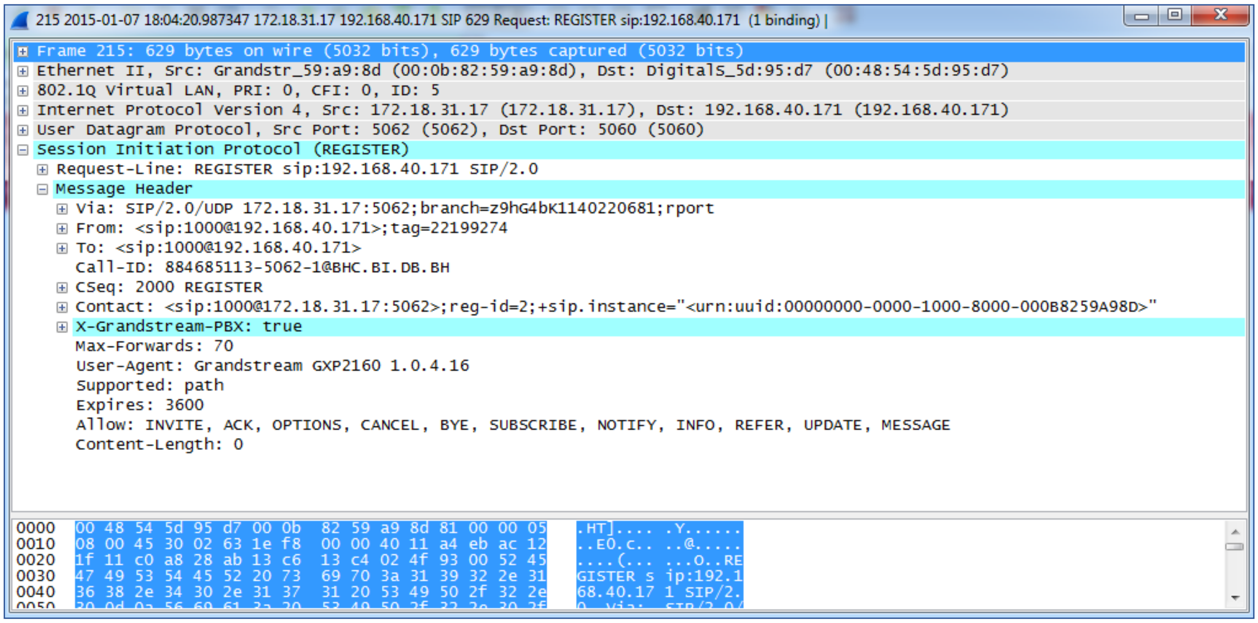
Figure 5: Strategy – Local Subnet Only

3. Save and Apply changes.

Now if the SIP end device is in subnet other than 192.168.40.x, e.g., 172.18.31.x subnet, the UCM will not allow registration using this extension. The following figure shows the SIP device IP address is 172.18.31.17. The UCM on IP 192.168.40.171 replies 404 Not Found for the registration request.



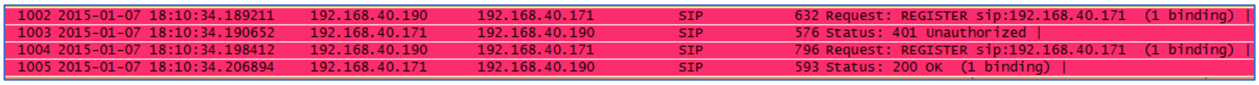
```
No.  Time                        Source           Destination      Protocol Length Info
 215 2015-01-07 18:04:20.987347  172.18.31.17     192.168.40.171   SIP         629 Request: REGISTER sip:192.168.40.171  (1 binding) |
 216 2015-01-07 18:04:20.989556  192.168.40.171   172.18.31.17     SIP         491 Status: 404 Not found |
 334 2015-01-07 18:04:42.194344  172.18.31.17     192.168.40.171   SIP         629 Request: REGISTER sip:192.168.40.171  (1 binding) |
 336 2015-01-07 18:04:42.196110  192.168.40.171   172.18.31.17     SIP         491 Status: 404 Not found |
 341 2015-01-07 18:05:03.242985  172.18.31.17     192.168.40.171   SIP         629 Request: REGISTER sip:192.168.40.171  (1 binding) |
 342 2015-01-07 18:05:03.244559  192.168.40.171   172.18.31.17     SIP         491 Status: 404 Not found |
```



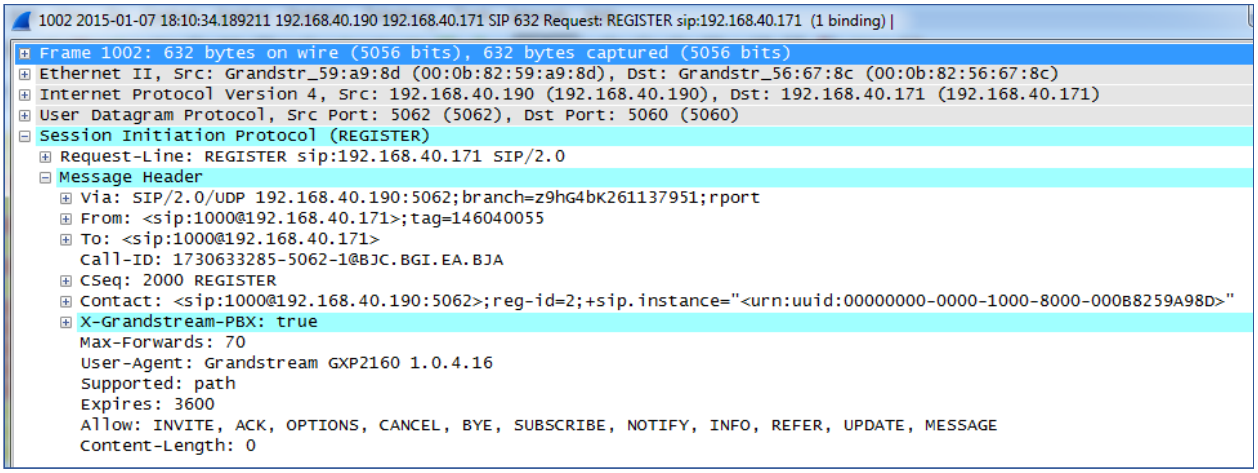
```
215 2015-01-07 18:04:20.987347 172.18.31.17 192.168.40.171 SIP 629 Request: REGISTER sip:192.168.40.171  (1 binding) |

⊞ Frame 215: 629 bytes on wire (5032 bits), 629 bytes captured (5032 bits)
⊞ Ethernet II, Src: Grandstr_59:a9:8d (00:0b:82:59:a9:8d), Dst: Digitals_5d:95:d7 (00:48:54:5d:95:d7)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 5
⊞ Internet Protocol Version 4, Src: 172.18.31.17 (172.18.31.17), Dst: 192.168.40.171 (192.168.40.171)
⊞ User Datagram Protocol, Src Port: 5062 (5062), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol (REGISTER)
  ⊞ Request-Line: REGISTER sip:192.168.40.171 SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 172.18.31.17:5062;branch=z9hG4bK1140220681;rport
    ⊞ From: <sip:1000@192.168.40.171>;tag=22199274
    ⊞ To: <sip:1000@192.168.40.171>
      Call-ID: 884685113-5062-1@BHC.BI.DB.BH
    ⊞ CSeq: 2000 REGISTER
    ⊞ Contact: <sip:1000@172.18.31.17:5062>;reg-id=2;+sip.instance="<urn:uuid:00000000-0000-1000-8000-000B8259A98D>"
    ⊞ X-Grandstream-PBX: true
      Max-Forwards: 70
      User-Agent: Grandstream GXP2160 1.0.4.16
      Supported: path
      Expires: 3600
      Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE
      Content-Length: 0

0000  00 48 54 5d 95 d7 00 0b  82 59 a9 8d 81 00 00 05   .HT]....  .Y......
0010  08 00 45 30 02 63 1e f8  00 00 40 11 a4 eb ac 12   ..E0.c..  ..@.....
0020  1f 11 c0 a8 28 ab 13 c6  13 c4 02 4f 93 00 52 45   ....(...  ...O..RE
0030  47 49 53 54 45 52 20 73  69 70 3a 31 39 32 2e 31   GISTER s  ip:192.1
0040  36 38 2e 34 30 2e 31 37  31 20 53 49 50 2f 32 2e   68.40.17  1 SIP/2.
0050  30 0d 0a 56 69 61 3a 20  53 49 50 2f 32 2e 30 2f   0..Via:   SIP/2.0/
```

Figure 6: Registration Failed from Subnet Not Allowed for Registration

Once moving this device to 192.168.40.x subnet, registration will be successful. The following figure shows the IP address for the same SIP end device is 192.168.40.190. The UCM on IP address 192.168.40.171 replies 200 OK for the registration request.



```
1002 2015-01-07 18:10:34.189211   192.168.40.190   192.168.40.171   SIP   632 Request: REGISTER sip:192.168.40.171  (1 binding) |
1003 2015-01-07 18:10:34.190652   192.168.40.171   192.168.40.190   SIP   576 Status: 401 Unauthorized |
1004 2015-01-07 18:10:34.198412   192.168.40.190   192.168.40.171   SIP   796 Request: REGISTER sip:192.168.40.171  (1 binding) |
1005 2015-01-07 18:10:34.206894   192.168.40.171   192.168.40.190   SIP   593 Status: 200 OK  (1 binding) |
```

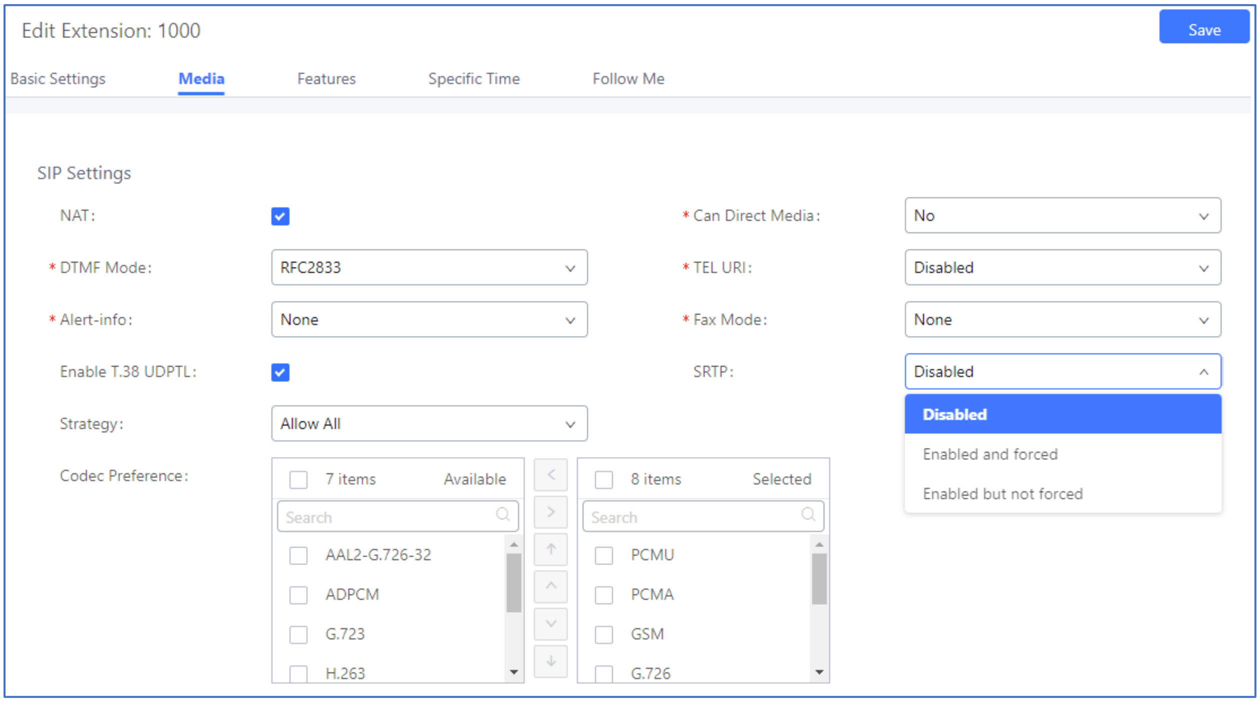


```
1002 2015-01-07 18:10:34.189211 192.168.40.190 192.168.40.171 SIP 632 Request: REGISTER sip:192.168.40.171  (1 binding) |

⊞ Frame 1002: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits)
⊞ Ethernet II, Src: Grandstr_59:a9:8d (00:0b:82:59:a9:8d), Dst: Grandstr_56:67:8c (00:0b:82:56:67:8c)
⊞ Internet Protocol Version 4, Src: 192.168.40.190 (192.168.40.190), Dst: 192.168.40.171 (192.168.40.171)
⊞ User Datagram Protocol, Src Port: 5062 (5062), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol (REGISTER)
  ⊞ Request-Line: REGISTER sip:192.168.40.171 SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.40.190:5062;branch=z9hG4bK261137951;rport
    ⊞ From: <sip:1000@192.168.40.171>;tag=146040055
    ⊞ To: <sip:1000@192.168.40.171>
      Call-ID: 1730633285-5062-1@BJC.BGI.EA.BJA
    ⊞ CSeq: 2000 REGISTER
    ⊞ Contact: <sip:1000@192.168.40.190:5062>;reg-id=2;+sip.instance="<urn:uuid:00000000-0000-1000-8000-000B8259A98D>"
    ⊞ X-Grandstream-PBX: true
      Max-Forwards: 70
      User-Agent: Grandstream GXP2160 1.0.4.16
      Supported: path
      Expires: 3600
      Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE
      Content-Length: 0
```

Figure 7: Registration Successful from Allowed Subnet

SRTP

SRTP is supported on UCM to secure RTP audio stream during the call. By default, it’s disabled. To use it, please configure under extension configuration dialog→“Media” tab when creating/editing an extension. If SRTP is enabled, RTP data flow will be encrypted.



Edit Extension: 1000

SIP Settings

NAT:	☑	* Can Direct Media:	No
* DTMF Mode:	RFC2833	* TEL URI:	Disabled
* Alert-info:	None	* Fax Mode:	None
Enable T.38 UDPTL:	☑	SRTP:	Disabled
Strategy:	Allow All		Disabled Enabled and forced Enabled but not forced
Codec Preference:	□ 7 items Available Search □ AAL2-G.726-32 □ ADPCM □ G.723 □ H.263		□ 8 items Selected Search □ PCMU □ PCMA □ GSM □ G.726

Figure 8: Enabling SRTP

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

- Enabled and forced: On this case, the extension does support SRTP for secure audio and doesn’t allow any calls without SRTP.
- Enabled But Not Forced: The extension does support SRTP, but can allow negotiation to setup calls without SRTP in case the other end doesn’t support it.

TRUNK SECURITY

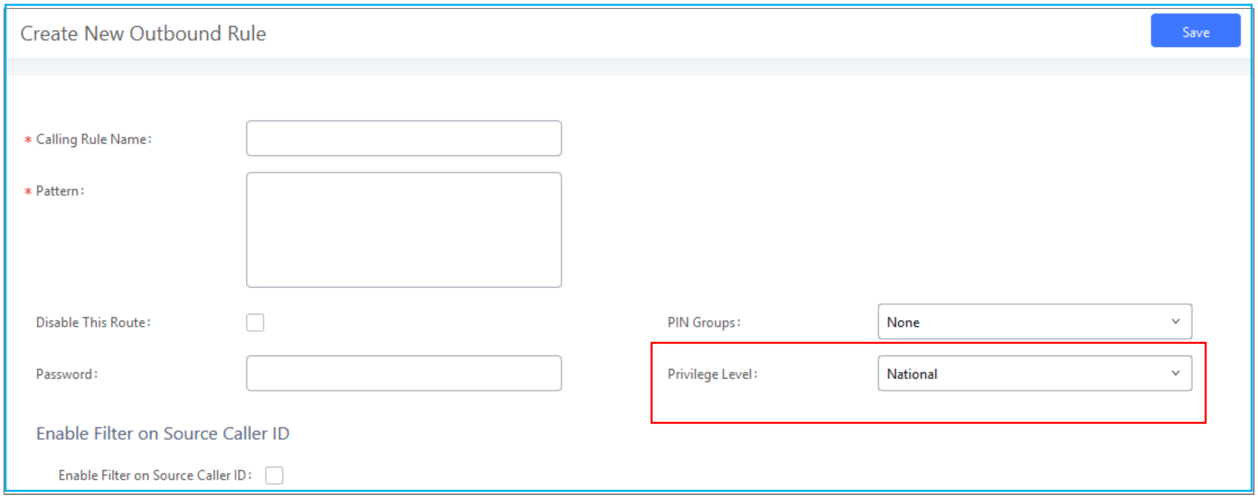
A potential risk for trunks is that unwanted users may gain the authority to make international or long-distance calls. This will result in unexpected high charges before the UCM administrator notices this. Usually this high cost is due to improper configurations on the UCM. Therefore, administrators must be extremely cautious when configuring those trunks that will be charged by placing certain calls, for example, PSTN trunks or SIP trunks with international call capability.

Outbound Rule Permissions

Four methods are supported on UCM to control outbound rule permissions and users can apply one of them to the outbound rule.

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

Please make sure to configure it to allow only the desired group of users to call from this route.



Create New Outbound Rule

* Calling Rule Name:			
* Pattern:			
Disable This Route:	□	PIN Groups:	None
Password:		Privilege Level:	National

Enable Filter on Source Caller ID

Enable Filter on Source Caller ID: □

Figure 9: Outbound Rule Permissions

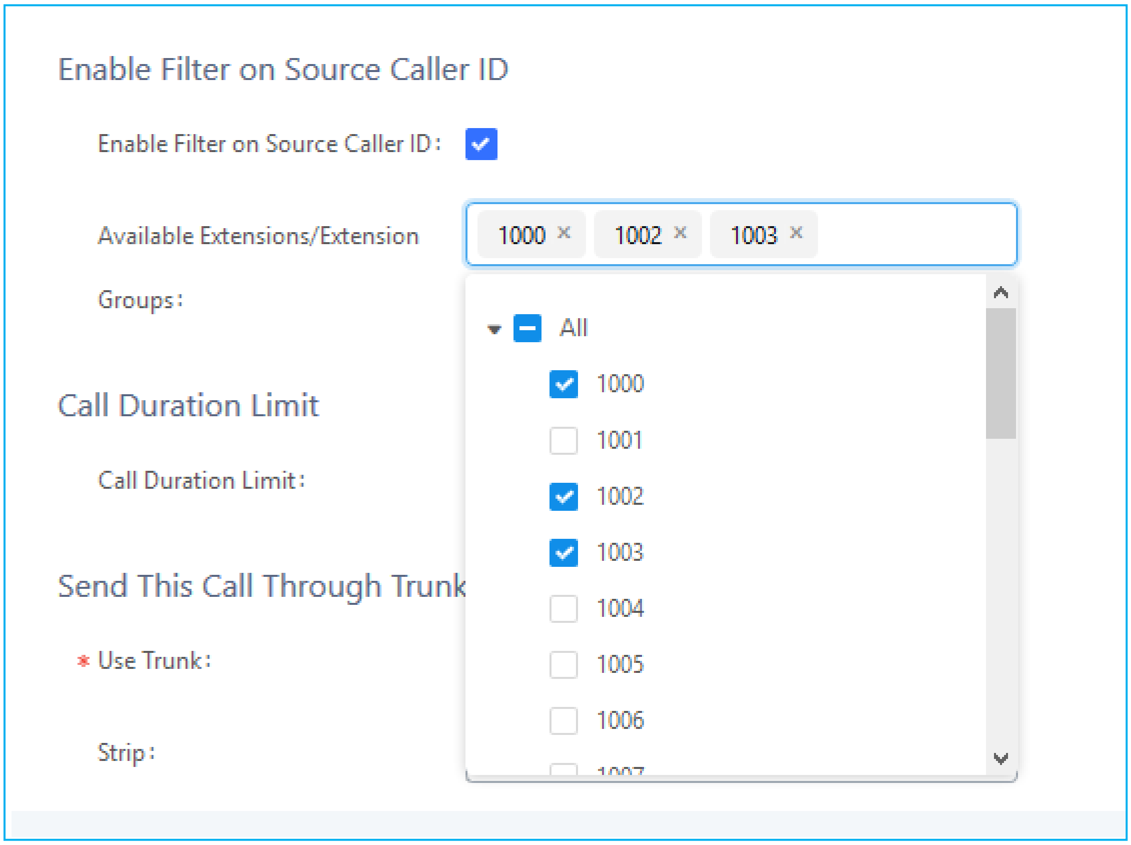
Privilege Level

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.

Please configure the privilege for the outbound rule high enough to restrict the extensions allowed to call external numbers via this trunk.

Source Caller ID Filter

Instead of using privilege level, UCM administrator could specify the extensions/extension groups that are allowed to use the outbound rule. This can be done by selecting extension/extension groups or defining pattern for the source caller ID in “Custom Dynamic Route” field. The extension allowed to make outbound call will either need to be an extension in the selected list or match the defined pattern.



Enable Filter on Source Caller ID

Enable Filter on Source Caller ID: ☑

Available Extensions/Extension Groups: 1000 × 1002 × 1003 ×

- All
- ☑ 1000
- □ 1001
- ☑ 1002
- ☑ 1003
- □ 1004
- □ 1005
- □ 1006
- □ 1007

Call Duration Limit

Call Duration Limit:

Send This Call Through Trunk

* Use Trunk:

Strip:

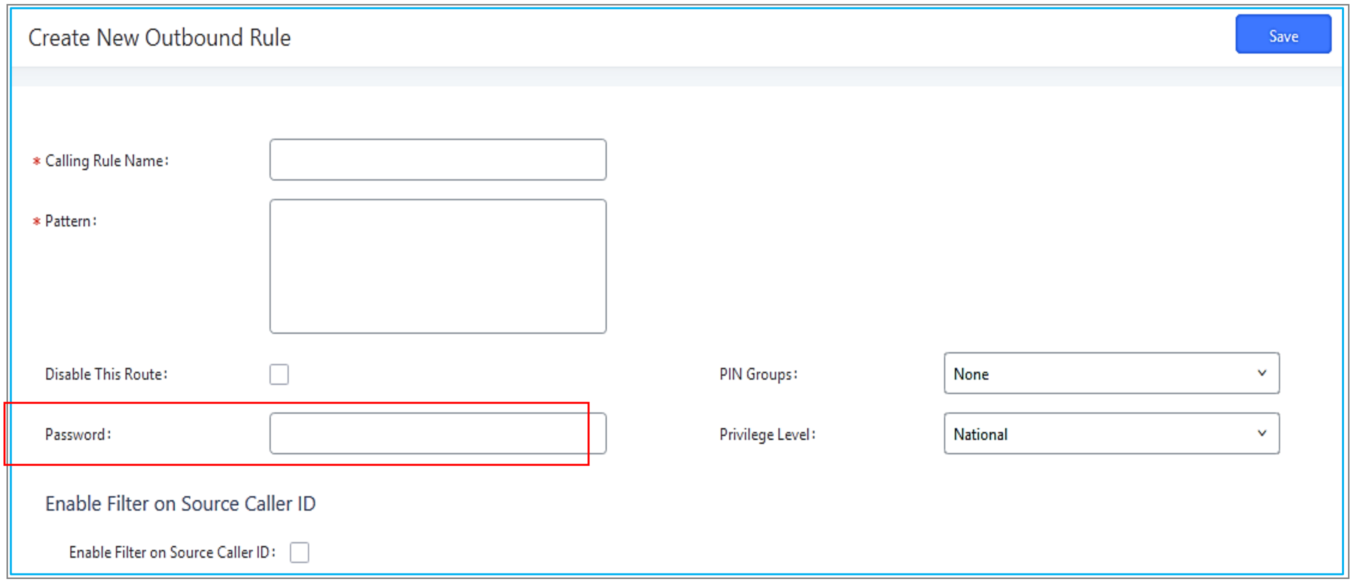
Figure 10: Source Caller ID Filter

Please specify the extension or the pattern here to the minimal set so that only the desired users can dial out from this outbound route.

For detailed configuration instructions, please refer to MANAGING OUTBOUND ROUTE section in white paper: How to manage inbound/outbound route on UCM6510/6100

Password protection

For even more security, users could protect the outbound rule with a password that will be requested by the UCM from the callers in order to allow outbound calls. Users can set the password on each outbound on the specified field as shown on the figure below.



Create New Outbound Rule

Save

* Calling Rule Name:

* Pattern:

Disable This Route: □

PIN Groups: None

Password:

Privilege Level: National

Enable Filter on Source Caller ID

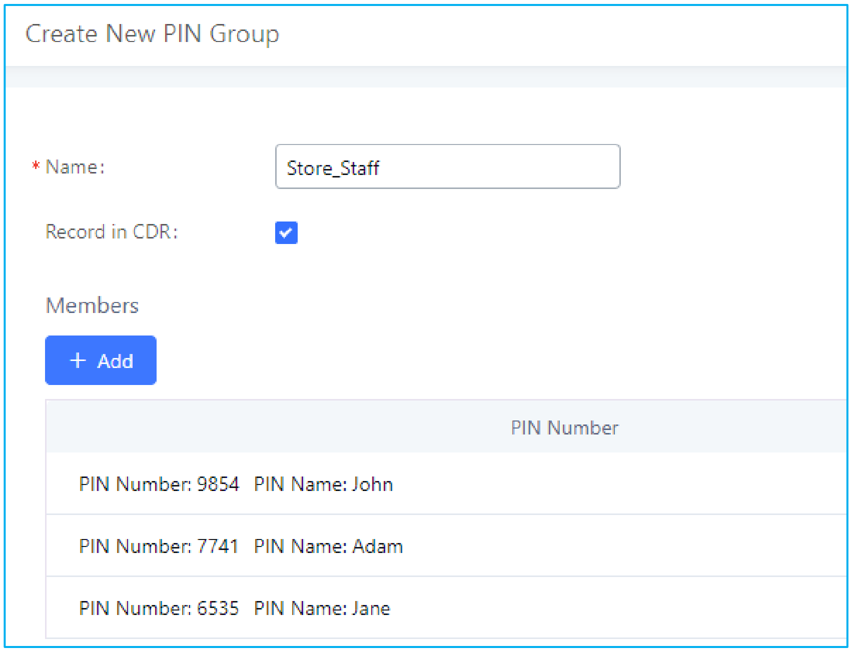
Enable Filter on Source Caller ID: □

Figure 11: Password Protection

PIN Groups

In some cases, multiple users do share same phone (ex: phone on public mode with user login), and the shared phone can be used to make outbound calls, the administrator on this case can set the outbound rule protection mode to PIN groups where each user should enter his PIN code in order to be allowed to make outbound calls through trunks. In order to set PIN group protection, the admin should follow below steps:

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



Create New PIN Group

* Name: Store_Staff

Record in CDR: ☑

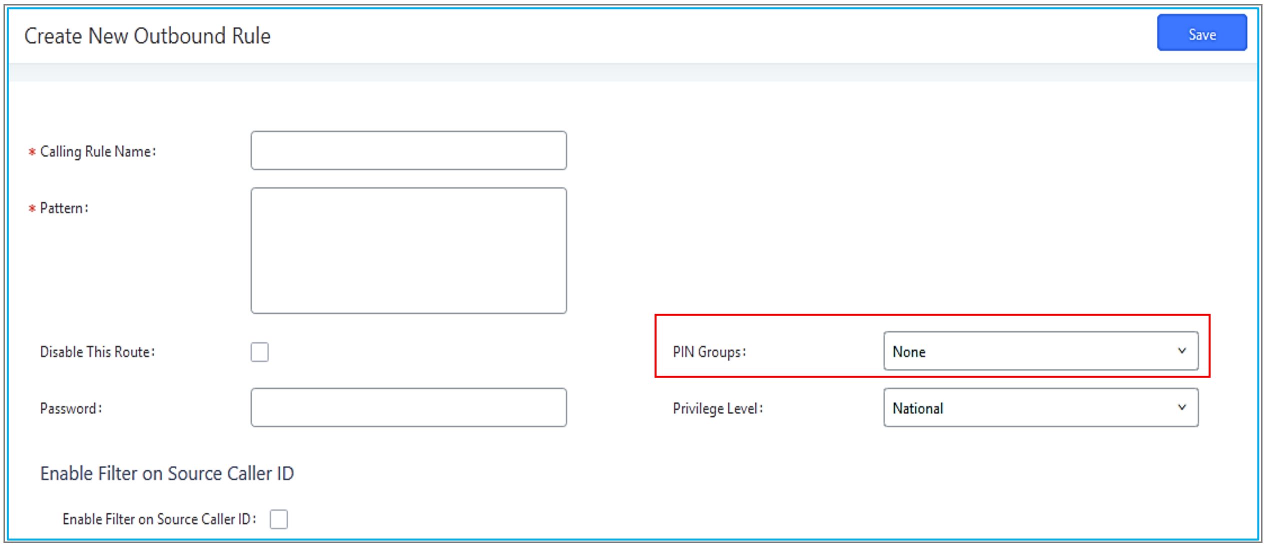
Members

+ Add

PIN Number
PIN Number: 9854 PIN Name: John
PIN Number: 7741 PIN Name: Adam
PIN Number: 6535 PIN Name: Jane

Figure 12: Adding PIN Groups

3. Save and apply, then on your outbound routes you can select the created group and each time one the PIN group members tries to make outbound call, he/she will be requested to enter their PIN code as a security protection.



Create New Outbound Rule

* Calling Rule Name:			
* Pattern:			
Disable This Route:	□	PIN Groups:	None
Password:		Privilege Level:	National

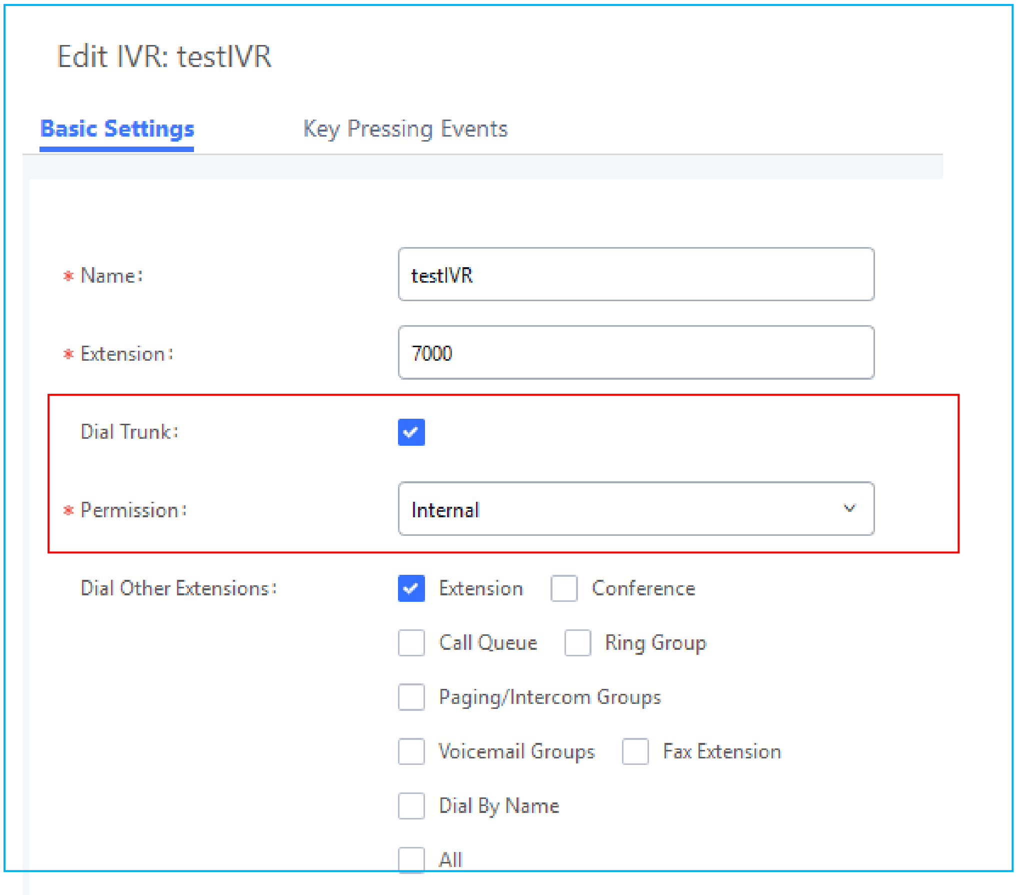
Enable Filter on Source Caller ID

Enable Filter on Source Caller ID: □

Figure 13: Outbound route with PIN group

IVR Dial Trunk

When creating/editing an IVR, the administrator could decide whether to allow the calls entering the IVR to make outbound calls through trunks by configuring “Dial Trunk” and “Permission”. If “Dial Trunk” option is enabled, the caller calling into the IVR will be able to dial external numbers through a trunk if the IVR’S permission is higher than or equal to the privilege of the trunk. The potential risk here is that unwanted users may call into IVR and then dial external number. This could possibly generate expected high charges especially if an IVR is configured as the destination of an inbound route of a PSTN trunk, in which case, anyone can call into the IVR and then dial out to long distance or international calls.



Edit IVR: testIVR

Basic Settings | Key Pressing Events

* Name: testIVR

* Extension: 7000

Dial Trunk: ☑

* Permission: Internal

Dial Other Extensions: ☑ Extension □ Conference □ Call Queue □ Ring Group □ Paging/Intercom Groups □ Voicemail Groups □ Fax Extension □ Dial By Name □ All

Figure 14: IVR Dial Trunk

We recommend disabling “Dial Trunk” option unless the risk associated with it is clearly understood or the PBX administrator intentionally configures it to do so for specific reasons. If it has to be enabled, please configure the “permission” as secure as possible to restrict the authorized callers to be known users.

For more information about IVR permissions, please refer to IVR PERMISSION section in white paper: [How to manage inbound/outbound route on UCM6510/6100]

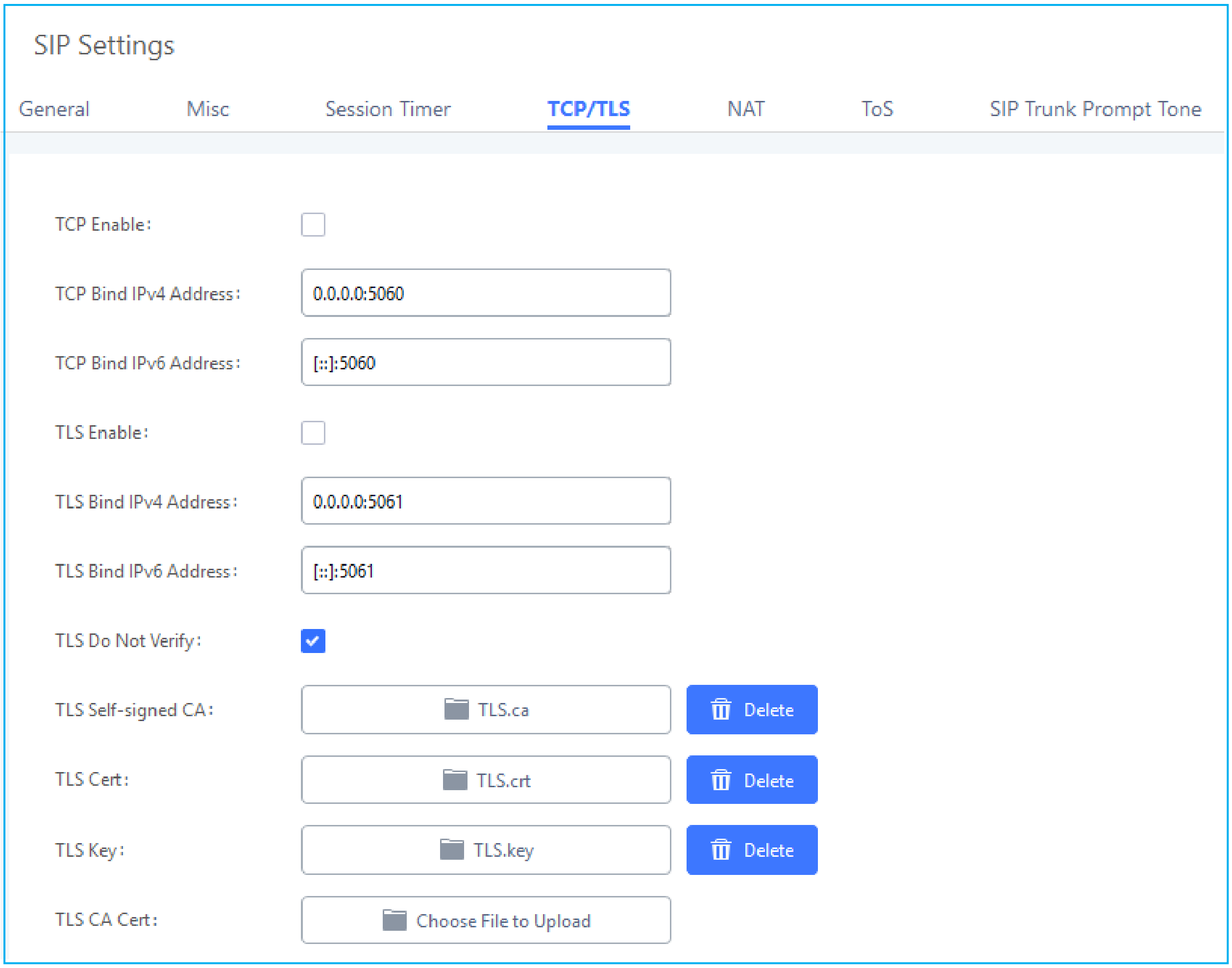
Allow Guest Calls

“Allow Guest Calls” option can be found on web GUI→PBX Settings→SIP Settings→General page. We highly recommend **NOT** to turn on this option for any deployments. Enabling “Allow Guest Calls” will stop the PBX from authenticating incoming calls from unknown or anonymous callers. In that case, hackers get the chance to send INVITE to UCM and the UCM will place the call without authentication. This can result in high toll charges. The administrator might also want to check CDR regularly to make sure there is no suspicious calls in the early stage of deployment.

TLS

The UCM administrators may consider securing SIP packets sent across an untrusted network. Using TLS could be a solution. It will authenticate servers and clients, and then encrypt SIP messages between the authenticated parties.

TLS can be configured under UCM web GUI→PBX Settings→SIP Settings→TCP/TLS page.



TCP Enable: □

TCP Bind IPv4 Address: 0.0.0.0:5060

TCP Bind IPv6 Address: [::]:5060

TLS Enable: □

TLS Bind IPv4 Address: 0.0.0.0:5061

TLS Bind IPv6 Address: [::]:5061

TLS Do Not Verify: ☑

TLS Self-signed CA: TLS.ca Delete

TLS Cert: TLS.crt Delete

TLS Key: TLS.key Delete

TLS CA Cert: Choose File to Upload

Figure 15: PBX Settings→SIP Settings→TCP/TLS

1. Set “TLS Enable” as “Yes” to enable TLS on UCM.
2. Configure “TLS Do Not Verify”, “TLS Self-Signed CA” and “TLS Cert” properly to achieve basic TLS authentication and encryption.

- **TLS Self-Signed CA**

  This is used when UCM acts as a client, to authenticate the server. If the server the UCM connecting to uses a self-signed certificate, you should have their certificate installed here so authenticity of their certificate can be verified. If the server uses a certificate that is signed by one of the larger CAs, you should install a copy of server CA certificate here.

- **TLS Cert**

  This is used when UCM acts as a server. It's sent to the client during TLS handshake. The TLS Cert should include the key and server certificate. The "common name" field in the server certificate should match the server host (either IP or domain name). This is required if the client side is another UCM (not a standard, some clients do not have this requirement for server authentication). If not matching, authentication on the UCM (client) fails and the TLS connection cannot get established.

- **TLS Do Not Verify**

  This is effective when UCM acts as a client. If set to "Yes", the server's certificate (sent to the client during TLS Handshake) won't be verified. Considering if two UCMs are peered, since the default certificate built in UCM at the factory has "common name" equaling "localhost" which is not a valid IP address, authentication will fail for sure. So, this is the default setting to avoid authentication failure when using default certificate. Please note skipping verification won't have effect on encrypting SIP messages. If set to "No", UCM (client) will verify the server's certificate using "TLS Self-Signed CA".

Please note that administrator also needs configure "SIP Transport" to be "TLS" on the SIP endpoint device to encrypt SIP messages sent to the UCM.

FIREWALL

The firewall functionality provided by UCM model consists of Static defense, Dynamic defense and Fail2ban. User could manually configure each of the three options to block certain malicious attack.

Static Defense

It can be configured from Web UI→System Settings→Security Settings→Static Defense. One main purpose of static defense is using pre-configured filtering rules. Three type of filtering rules are supported, ACCEPT, REJECT, and DROP. UCM administrator can configure filtering rules based on source/destination IP addresses and ports. For example, if a remote host allowed to connect to a certain service using port X is known with IP x.x.x.x, the administrator can create an ACCEPT rule to allow traffic from IP x.x.x.x destined to port X on UCM.

The options to configure static defense rule are as follows:

- Rule Name: Created by user to identify this rule.
- Action: Accept, Reject or Drop depending on how the user would like the rule to perform.
- Type: In/out indicates the traffic direction.
- Interface: Select network interface where the traffic will go through.
- Service: Users can select the pre-defined service (FTP/SSH/Telnet/TFTP/HTTP/LDAP) or “Custom” which allows a specific restriction. If “Custom” is selected, please define source and destination IP address + Port. Users need to select “Protocol” as TCP, UDP or Both.

In addition, Static Defense also provides three pre-configured defense mechanisms:

1. Ping Defense

Once enabled, ICMP response will not be allowed for Ping request. This is a predefined mechanism in order to protect flooding Ping attack.

2. SYN-Flood Defense

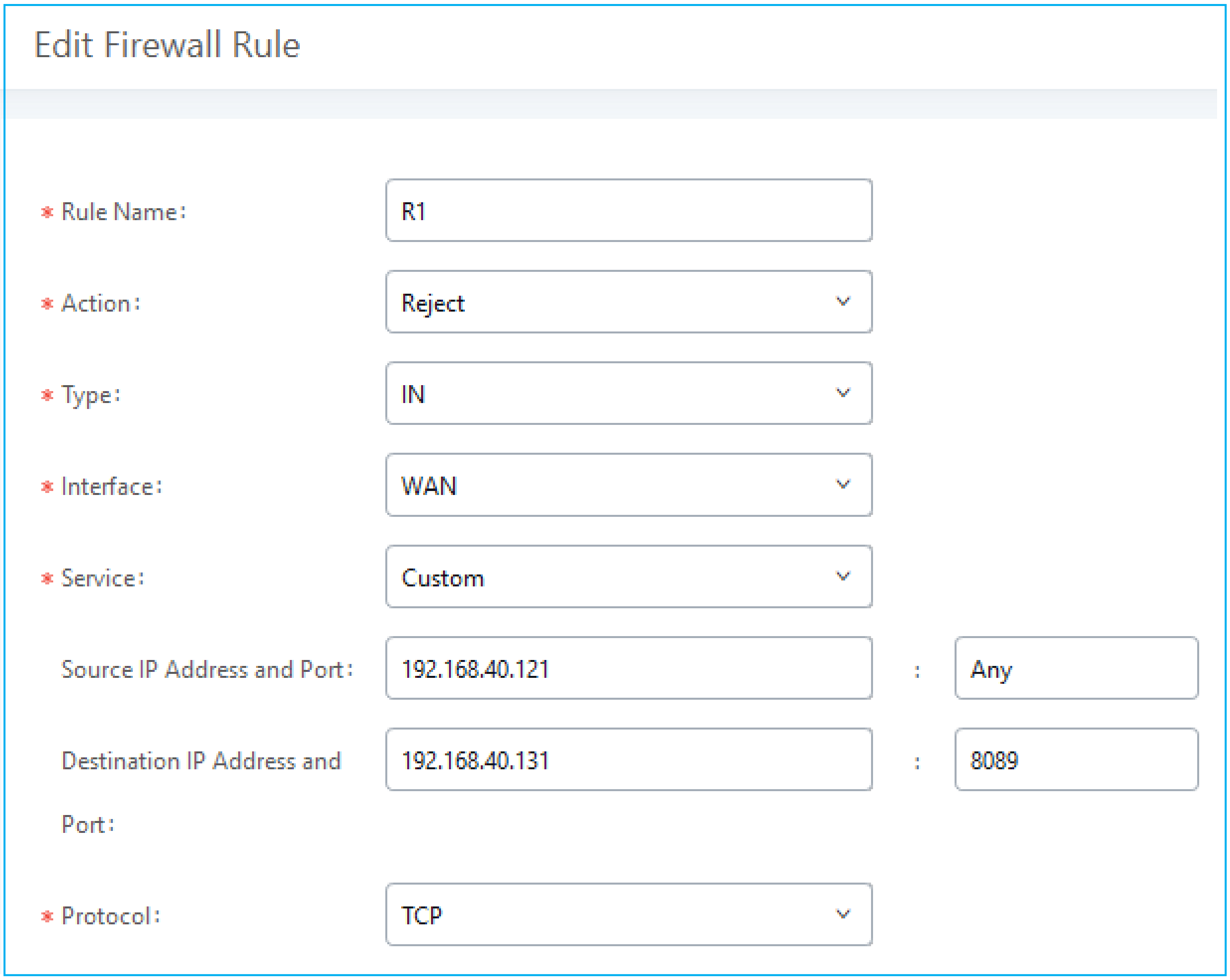
Once enabled, UCM can response to the SYN flood denial-of-service (DOS) attack.

3. Ping-of-Death defense

Once enabled, UCM can response to the Ping packet that is greater than 65,536 bytes.

Static Defense Example: Blocking TCP Connection from a Specific Host

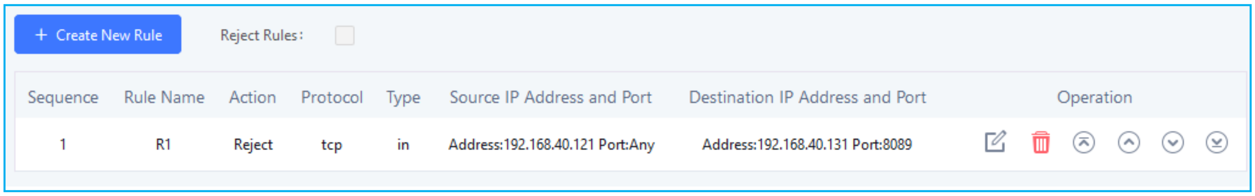
This example demonstrates how to set up a new rule to block a host with a specific IP address to connect to UCM using TCP connection. In the following figure, 192.168.40.142 is the host IP address and 192.168.40.131 is the UCM's IP address. Port 8089 on UCM is used for HTTP server/web UI access. This setting will block host on 192.168.40.131 to access UCM port 8089 using TCP connection.



Edit Firewall Rule

* Rule Name:	R1		
* Action:	Reject		
* Type:	IN		
* Interface:	WAN		
* Service:	Custom		
Source IP Address and Port:	192.168.40.121	:	Any
Destination IP Address and Port:	192.168.40.131	:	8089
* Protocol:	TCP		

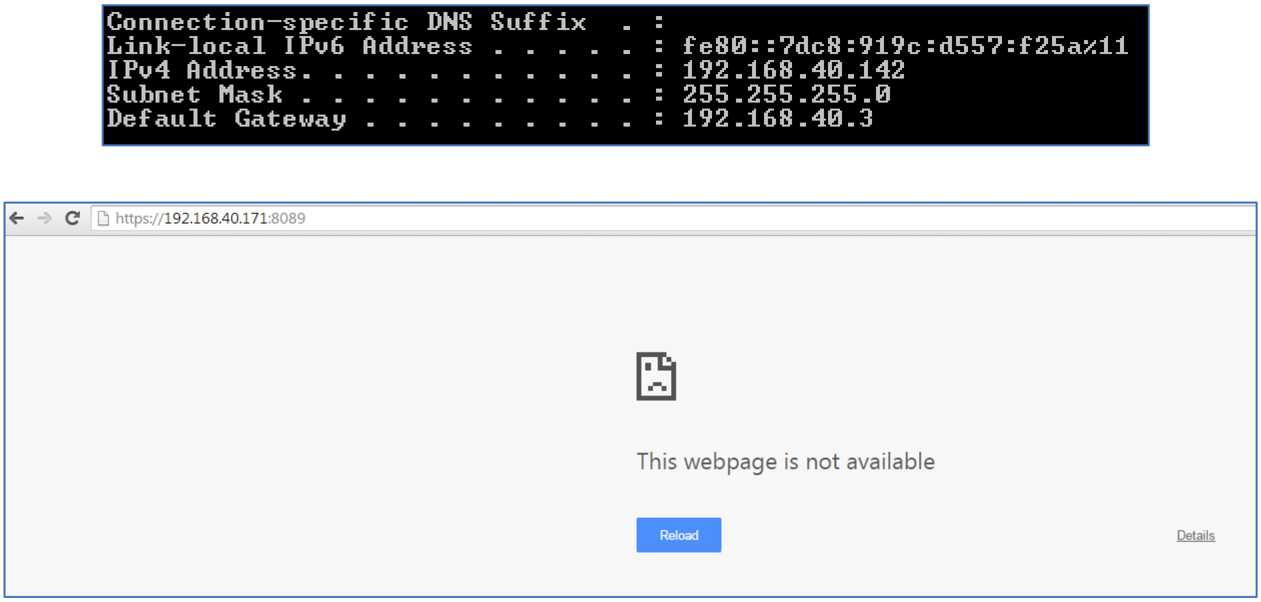
Figure 16: Firewall Rule Custom Configuration



Sequence	Rule Name	Action	Protocol	Type	Source IP Address and Port	Destination IP Address and Port	Operation
1	R1	Reject	tcp	in	Address:192.168.40.121 Port:Any	Address:192.168.40.131 Port:8089	

Figure 17: Static Defense Blocking Host 192.168.40.142 Using TCP Connection

After saving and applying the change, host 192.168.40.142 will not be able to access UCM web UI anymore.



```
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::7dc8:919c:d557:f25a%11
IPv4 Address. . . . . . . . . . . : 192.168.40.142
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.40.3
```

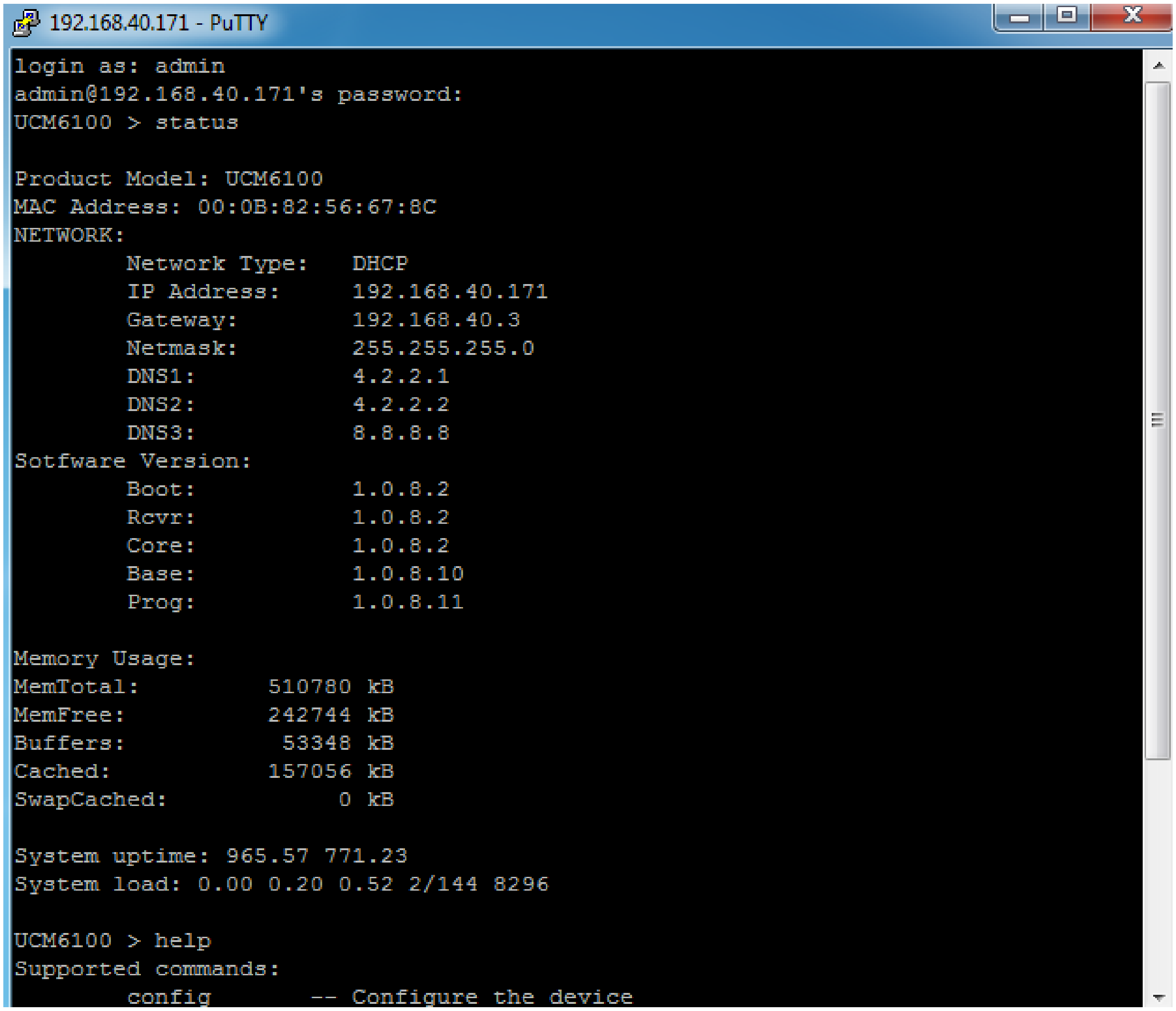
https://192.168.40.171:8089

This webpage is not available

Figure 18: Host blocked by UCM

Static Defense Example: Blocking SSH Connection to UCM

The UCM can be accessed via SSH connection by default. The SSH access provides device status information, reboot, reset and limited configuration capabilities. It is recommended to disable it once the UCM is deployed for security purpose. This can be done using static defense.



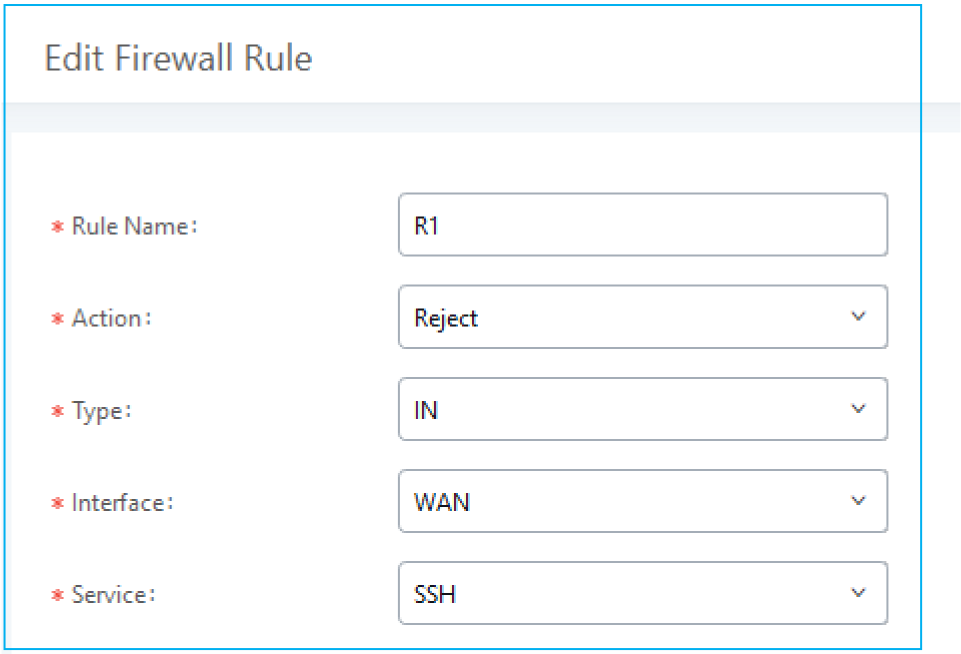
```
login as: admin
admin@192.168.40.171's password:
UCM6100 > status

Product Model: UCM6100
MAC Address: 00:0B:82:56:67:8C
NETWORK:
        Network Type:   DHCP
        IP Address:     192.168.40.171
        Gateway:        192.168.40.3
        Netmask:        255.255.255.0
        DNS1:           4.2.2.1
        DNS2:           4.2.2.2
        DNS3:           8.8.8.8
Sotfware Version:
        Boot:           1.0.8.2
        Rcvr:           1.0.8.2
        Core:           1.0.8.2
        Base:           1.0.8.10
        Prog:           1.0.8.11

Memory Usage:
MemTotal:          510780 kB
MemFree:           242744 kB
Buffers:            53348 kB
Cached:            157056 kB
SwapCached:             0 kB

System uptime: 965.57 771.23
System load: 0.00 0.20 0.52 2/144 8296

UCM6100 > help
Supported commands:
        config       -- Configure the device
```

Figure 19: UCM SSH Access

Configuration steps:

1. In UCM web UI→System Settings→Security Settings→Static Defense page, click on “Create New Rule”.

2. In the prompt window, configure the following parameters:
   Rule Name: Configure a name to identify this rule.
   Action: Reject.
   Type: IN.
   Interface: WAN (for UCM6202).
   Service: SSH.



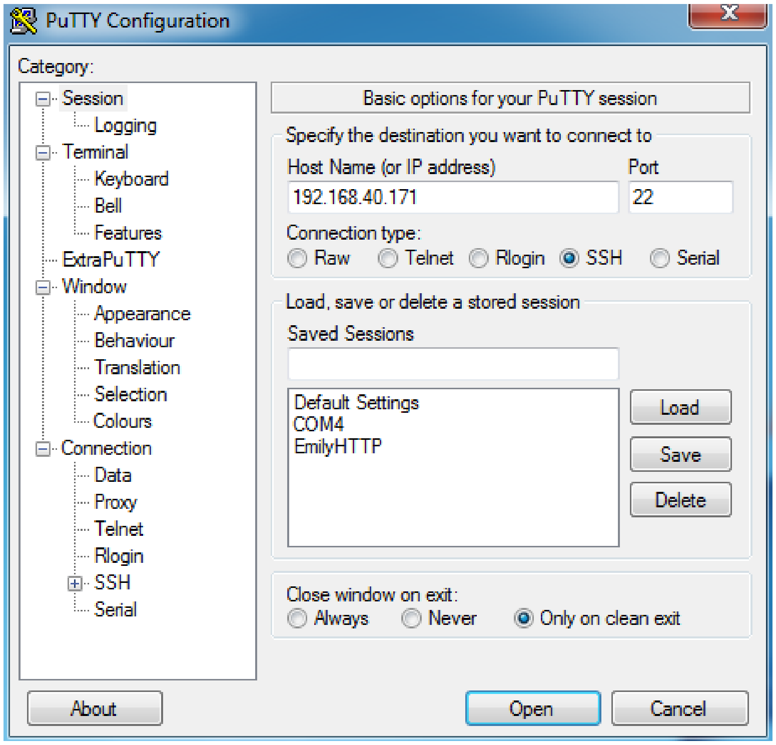
Edit Firewall Rule

- Rule Name: R1
- Action: Reject
- Type: IN
- Interface: WAN
- Service: SSH

Figure 20: Block SSH Connection

3. Save and apply changes.

Now SSH connection to the UCM will not be allowed anymore from any host.



PuTTY Configuration

Specify the destination you want to connect to

Host Name (or IP address): 192.168.40.171

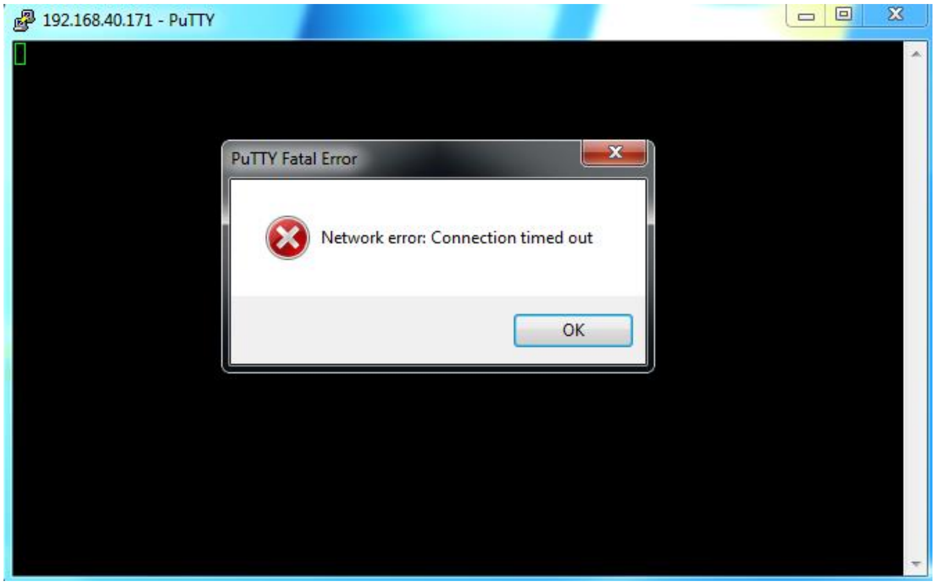
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions:
Default Settings
COM4
EmilyHTTP

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 21: Putty Setup for SSH Connection



Network error: Connection timed out

Figure 22: SSH Connection Blocked by UCM

Dynamic Defense

Dynamic defense is supported on UCM6102/UCM6202/UCM6204/UCM6208 and UCM6510 when LAN mode is set to "Route". It can be configured from Web UI→System Settings→Security Settings→Dynamic Defense. Once enabled, it will try to blacklist massive connection attempts or brute force attacks made by individual host.

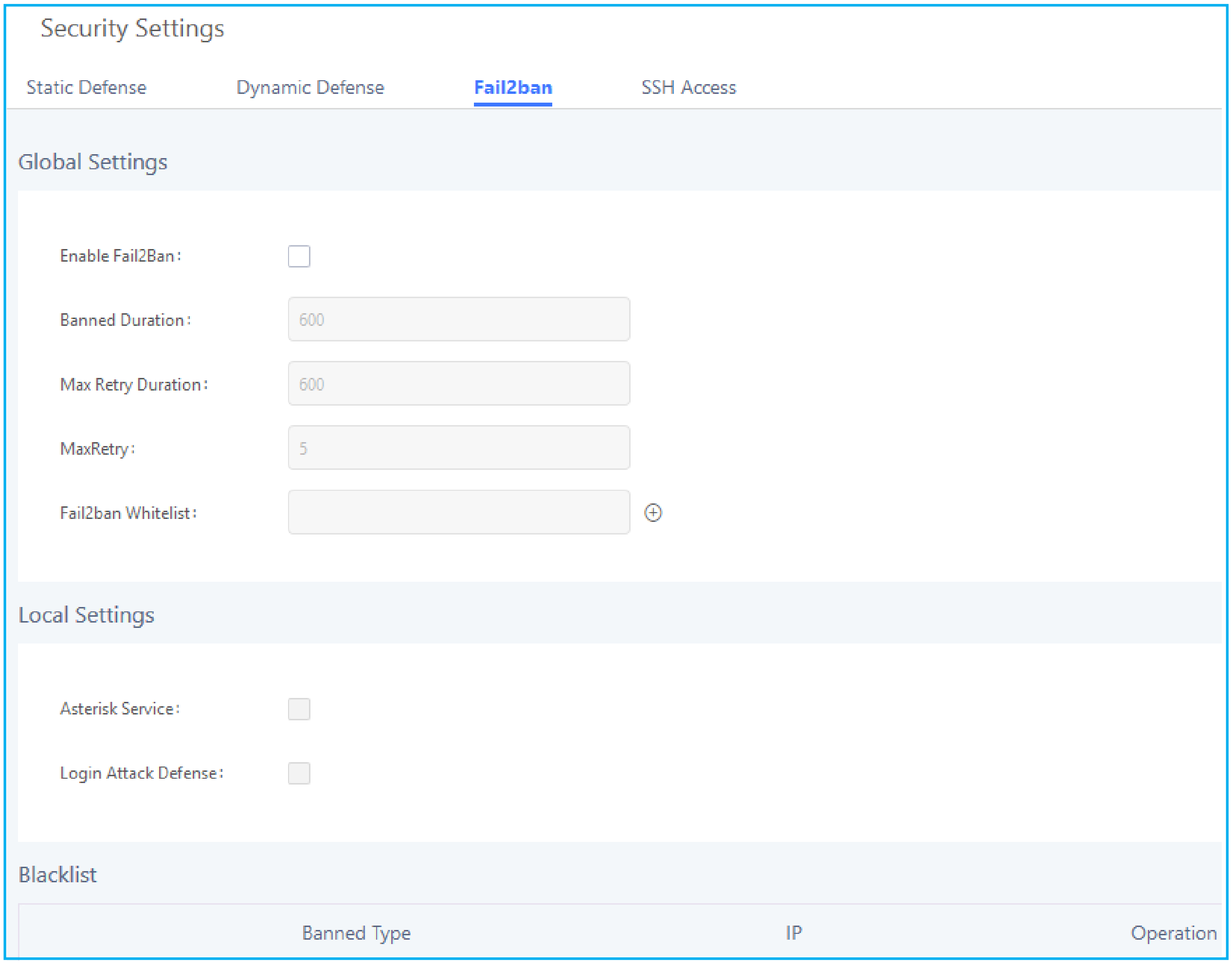
The UCM Dynamic Defense model also allows users to customize the connection threshold and time interval, meaning users can manually set the period for the max connection made by individual IP address. In addition, whitelist is supported so that certain hosts will not be blocked by Dynamic Defense.

For more configuration details, please refer to UCM User Manual.

Fail2ban

Fail2Ban is mainly designed to detect and prevent intrusion for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE method. It can be configured from Web UI→System Settings→Security Settings→Fail2ban. Users can customize the maximum retry times that one host can attempt in a period of time. If a host initiates attempts which exceed maximum retry times, it will be banned by UCM for a certain amount of time. User can also add a whitelist for the host that will not be punished by this defensive mechanism.

Fail2Ban can be enabled in the UCM web UI→System Settings→Security Settings→Fail2Ban. By default, Fail2Ban is disabled (see figure below).



Security Settings

Static Defense | Dynamic Defense | **Fail2ban** | SSH Access

Global Settings

Enable Fail2Ban : □

Banned Duration : 600

Max Retry Duration : 600

MaxRetry : 5

Fail2ban Whitelist : ⊕

Local Settings

Asterisk Service : □

Login Attack Defense : □

Blacklist

Banned Type	IP	Operation

Figure 23: Fail2Ban Default Configuration

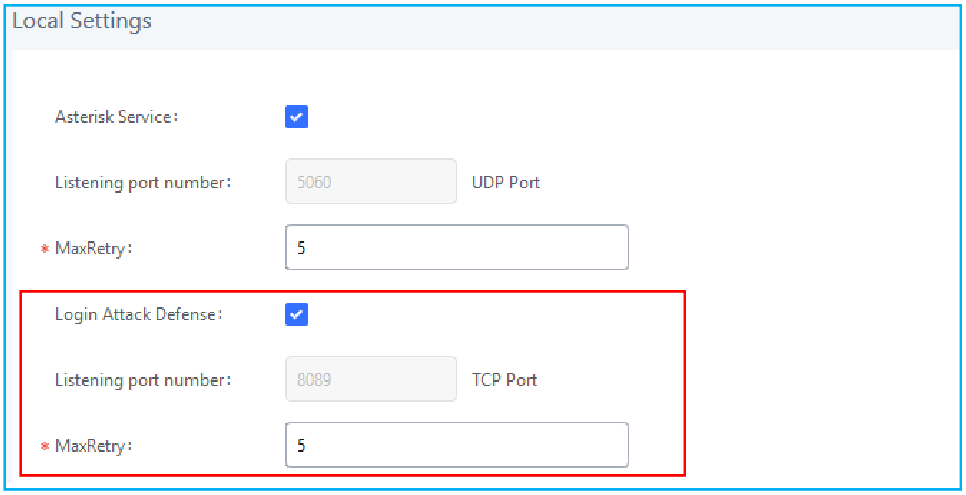
Enable Fail2Ban: Check it to enable Fail2Ban on the UCM.

Banned Duration: This specifies the amount of time the IP address will be blocked by UCM. By default, it is set to 10 mins (600s).

Max Retry Duration: This specifies the amount of time one IP host can connect to the UCM. If in this period the host connection exceeds the maximum connection limit, it will be banned for the “Banned Duration”. By default, it is set to 10 mins (600s).

Max Retry: This speficies the amount of times a host can try to connect to the UCM during “Max Retry Duration. If the host connection exceeds this limit within Max Retry Duration, it will be banned for the “Banned Duration”. By default, it is set to 5 times.

Fail2Ban Whitelist: user can add desired IP address into the whiltelist in order to bypass this restriction. By default, 127.0.0.1/8 is set to the loopback address.



Local Settings

Asterisk Service: ☑

Listening port number: 5060 UDP Port

* MaxRetry: 5

Login Attack Defense: ☑

Listening port number: 8089 TCP Port

* MaxRetry: 5

Figure 24: Asterisk Service Fail2Ban setting

If Fail2Ban is enabled under “Global Settings”, user must select “Asterisk Service” under “Local Settings” in order for it to take effect. Starting from firmware version 1.0.15.13, UCM Fail2ban feature works on all type of ports (UDP, TCP and TLS). Users can then define the value for “MaxRetry” which will override the "MaxRetry" value under "Global Settings". “Max Retry” specifies the number of authentication failures during "Max Retry Duration" before the host is banned and the default value is 5.

In addition to defending against hostile SIP messages, Fail2Ban can now be configured to defend against login attacks. Excessive login attempts will ban IP addresses from accessing the UCM web UI, users could enable the option as shown on the figure above.

Once enabled, and When the number of failed login attempts from an IP address exceeds the MaxRetry number, that IP address will be banned from accessing the UCM Web UI.

Please note the listening port number is always kept the same as HTTP server number under UCM web UI →Menu→System Settings→HTTP Server→Port.

AMI

Asterisk Manager Interface (AMI) is supported on UCM with restricted access. The documentation can be found in the following link:

http://www.grandstream.com/products/ucm_series/UCM/documents/UCM_ami_guide.pdf

Please do not enable AMI on the UCM if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your UCM system. Please be cautious when enabling AMI access on the UCM and restrict the permission granted to the AMI user.

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