Grandstream Networks, Inc.

UCM6100 Security Manual

Index

Table of Contents

Table of Figures

OVERVIEW

This document presents a summary of security concerns on UCM6100. It covers the security risks and related configurations that users need to consider when deploying the UCM6100.

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 UCM6100 against malicious attacks: Static Defense, Dynamic Defense (UCM6510 and UCM6102 only) and Fail2ban.

- **AMI**
  Using AMI feature comes with security concerns for UCM6100 administrators to consider.

WEB UI ACCESS

UCM6100 HTTP SERVER ACCESS

The UCM6100 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 UCM6100. 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 UCM6100 on public network could expose the domain name / IP address of the UCM6100 and pose serious security concerns.

PROTOCOL TYPE

HTTP and HTTPS (default) are supported to access the UCM6100 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 UCM6100. Therefore, it's recommended to use HTTPS instead of HTTP to secure the transactions and prevent unauthorized access.

USER LOGIN

UCM6100 web UI access is restricted by user login. Username and password are required when logging in to web UI.

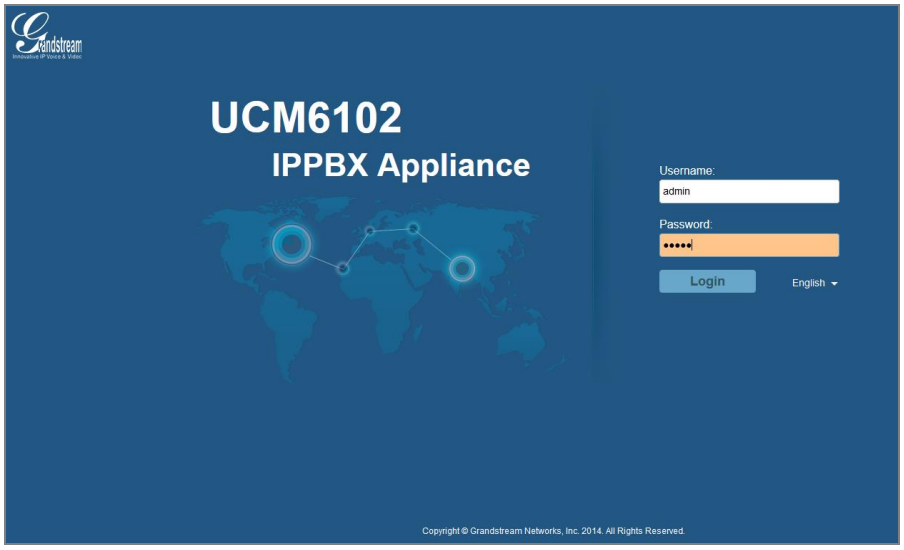


Figure 1: UCM6102 Web UI Login

The factory default value of “Username” and “Password” is “admin” and “admin”. 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 TIMEOUT

An authenticated user of the UCM6100 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 UCM6100, meaning all the configuration and status information could be exposed and changed intentionally or unintentionally.

UCM6100 provides protection from such vulnerability using login timeout. After the user logs in the UCM6100 web UI, the user will be automatically logged out after certain timeout. This timeout value can be specified under UCM100 web GUI->Settings->Login Timeout 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.

TWO-LEVEL USER MANAGEMENT

On UCM6100, two privilege levels for web UI users are supported:

- **Super Admin**: high priority
- **Admin**: low priority

Super administrator can access all pages on UCM6100 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 UCM6100 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 UCM6100 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 privilege "Admin".

Super Admin also has the authority to view operations done by all the users in web GUI->Settings->User Management->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 UCM6100 in your enterprise, it's highly recommended for the super administrator to create lower privilege administrators in order to manage the UCM6100 together, instead of handing out super administrator password to all the other users who may need access the UCM6100 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.

EXTENSION SECURITY

SIP/IAX PASSWORD

When creating a new SIP/IAX extension, the UCM6100 administrator is required to configure "SIP/IAX Password" which will be used for account registration authentication.

If "Enable Random Password" (on web GUI->PBX->Internal Options->General) is enabled, "SIP/IAX Password" is automatically filled with a randomly generated secure password when creating the extension on the UCM6100.

If "Enable Strong Password" (on web GUI-> **PBX**->**Internal Options**->**General**) 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 UCM6100 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 UCM6100 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 UCM6100.

2. Under UCM6100 web UI extension dialog, configure “Local Subnet Only” for “Strategy” option and 192.168.40.0 for “Local Subnet”.

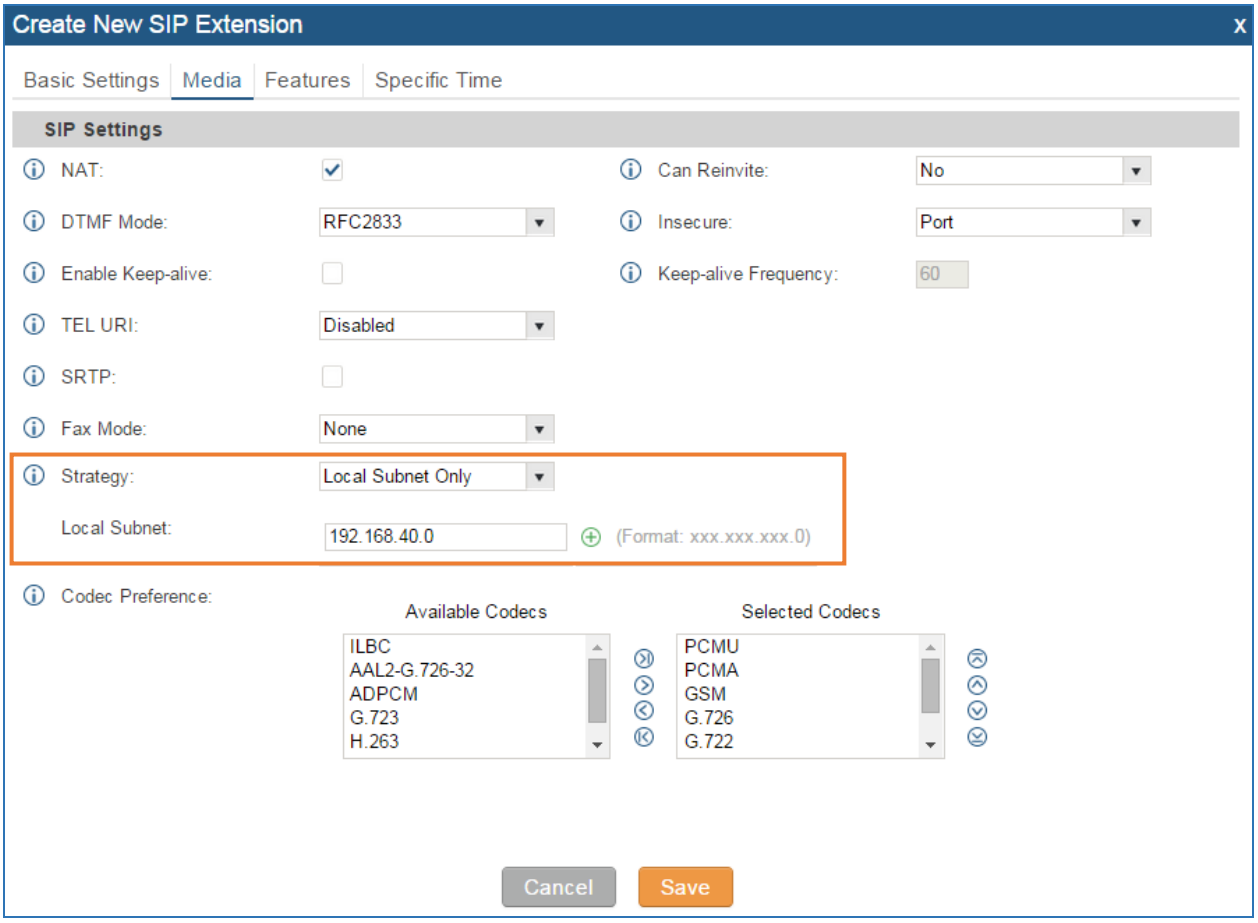


Figure 2: Strategy – Local Subnet Only

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 UCM6100 will not allow registration using this extension. The following figure shows the SIP device IP address is 172.18.31.17. The UCM6100 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 |

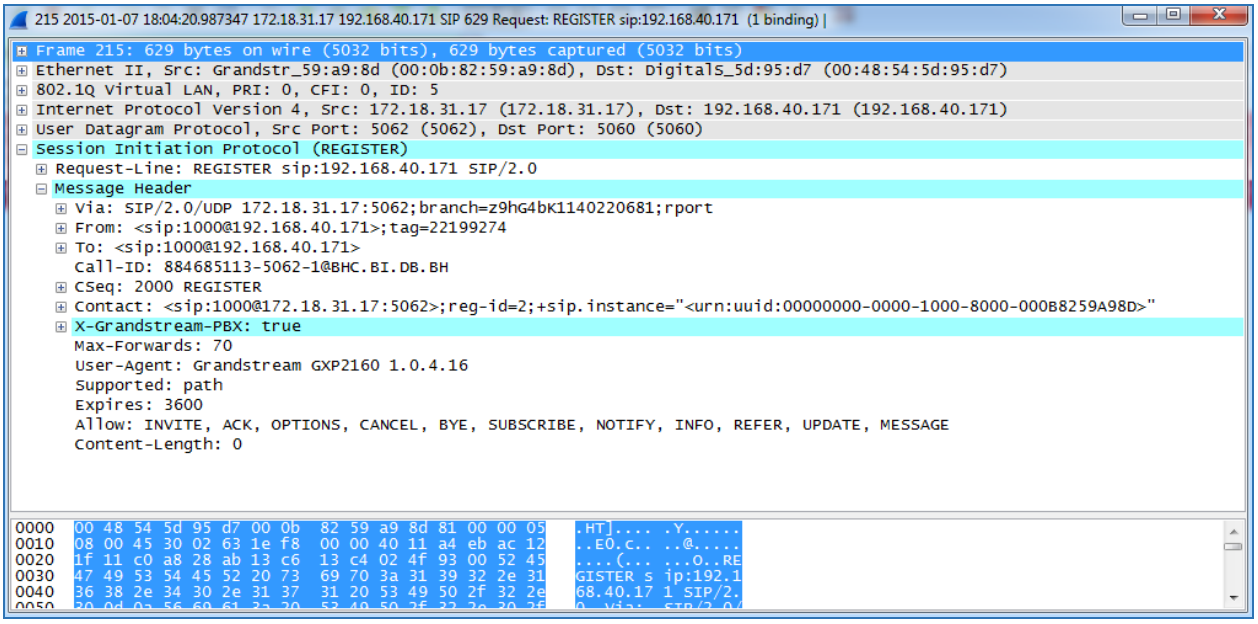
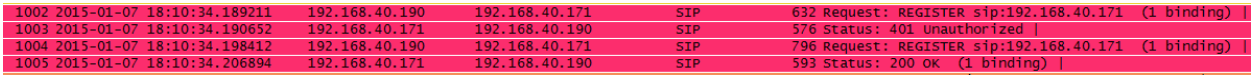


Figure 3: Registration Failed From Subnet Not Allowed For Registration

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 UCM6100 on IP address 192.168.40.171 replies 200 OK for the registration request.



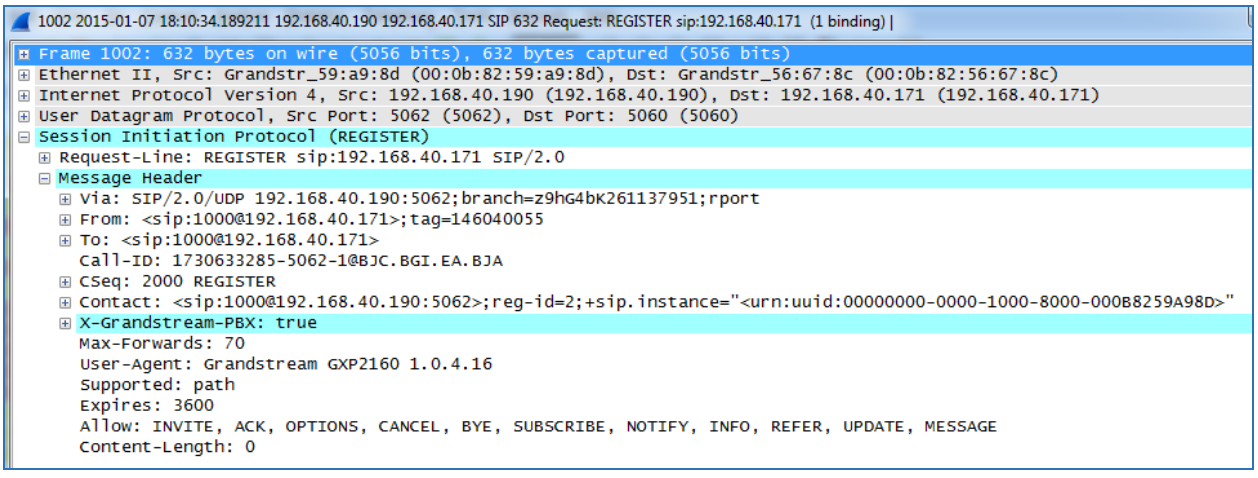


Figure 4: Registration Successful From Allowed Subnet

SRTP

SRTP is supported on UCM6100 to secure RTP during the call. By default it's disabled. To use it, please configure under extension configuration dialog->"Media" tag when creating/editing an extension. If SRTP is enabled, RTP data flow will be encrypted.

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 UCM6100 administrator notices this. Usually this high cost is due to improper configurations on the UCM6100. 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

Two methods are supported on UCM6100 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

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

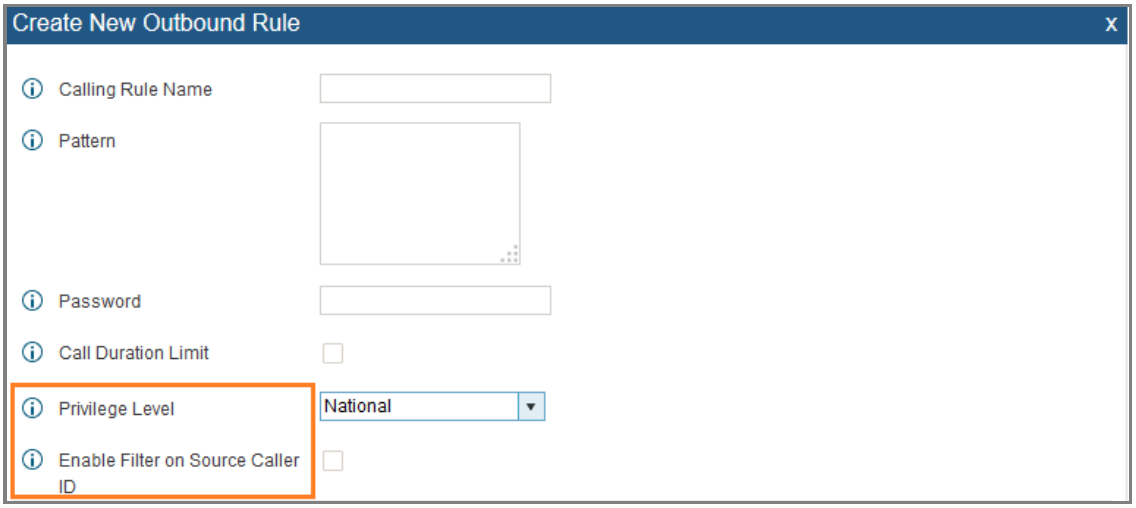


Figure 5: Outbound Rule Permissions

PRIVILEGE LEVEL

On the UCM6100, 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 privilege of the caller is higher or equal to the privilege 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, UCM6100 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.

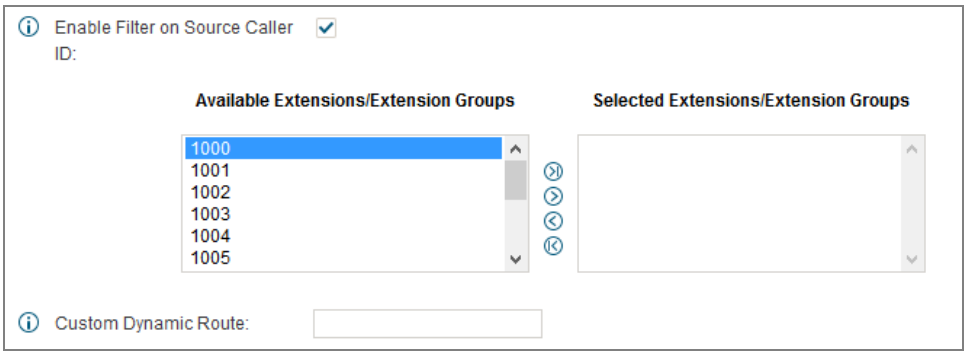


Figure 6: Source Caller ID Filter

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]

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.

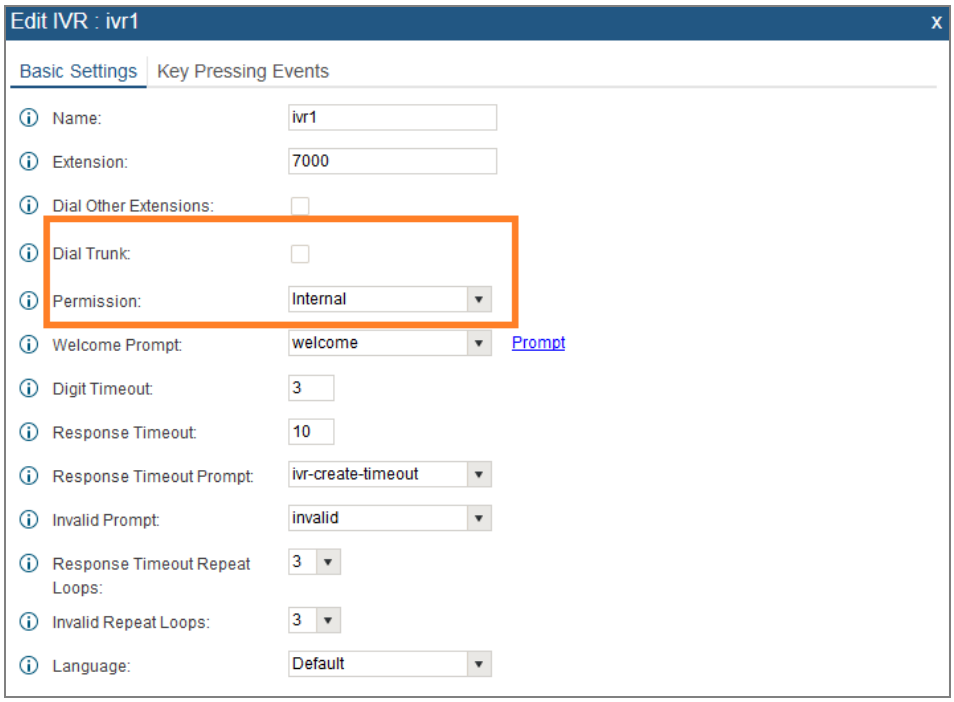


Figure 7: IVR Dial Trunk

We recommend to disable "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->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 UCM6100 and the UCM6100 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 UCM6100 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 UCM6100 web GUI->PBX->SIP Settings->TCP/TLS page.

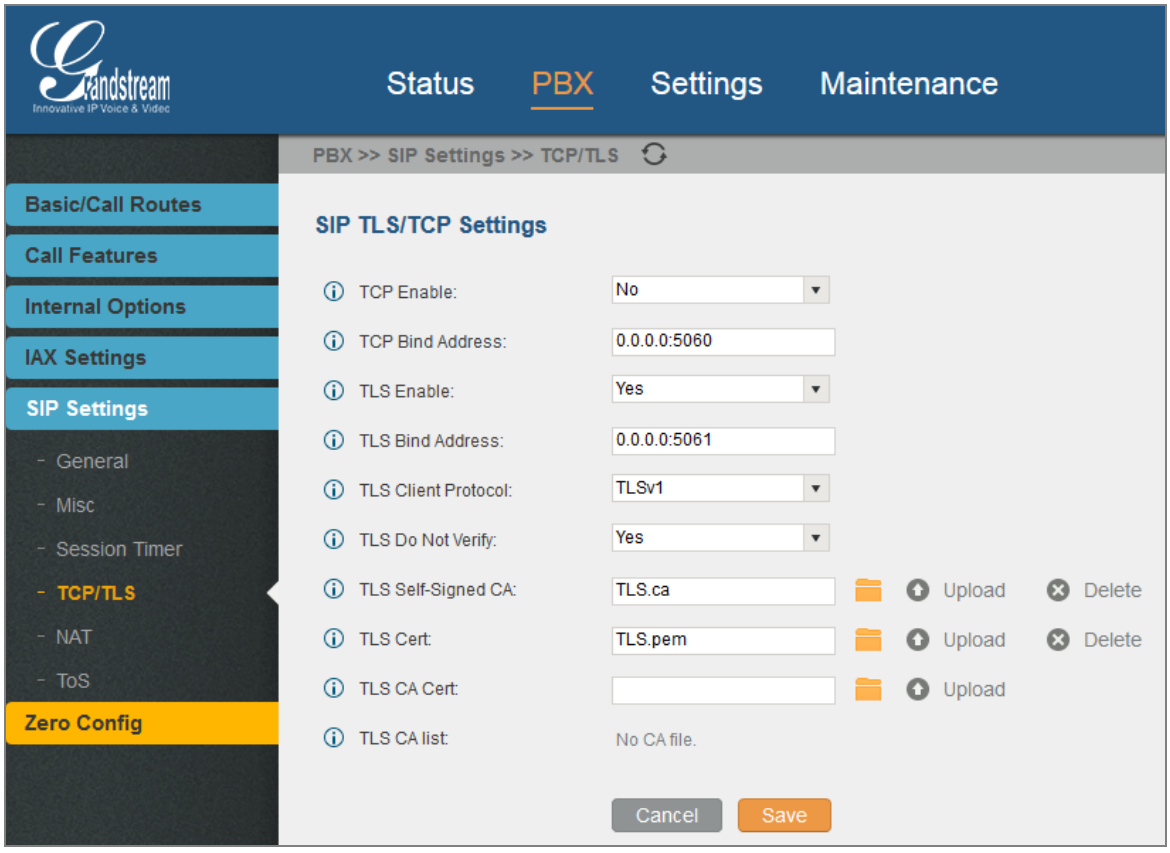


Figure 8: PBX->SIP Settings->TCP/TLS

1. Set “TLS Enable” as “Yes” to enable TLS on UCM6100.
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 UCM6100 acts as a client, to authenticate the server. If the server the UCM6100 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 UCM6100 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 UCM6100 (not a standard, some clients do not have this requirement for server authentication). If not matching, authentication on the UCM6100 (client) fails and the TLS connection cannot get established.

- **TLS Do Not Verify**

  This is effective when UCM6100 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 UCM6100s are peered, since the default certificate built in UCM6100 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", UCM6100 (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 UCM6100.

FIREWALL

The firewall functionality provided by UCM6100 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->Settings->Firewall->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. UCM6100 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 UCM6100.

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 mechanism:

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, UCM6100 can response to the SYN flood denial-of-service (DOS) attack.

3. Ping-of-Death defense

Once enabled, UCM6100 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 UCM6100 using TCP connection. In the following figure, 192.168.40.142 is the host IP address and 192.168.40.131 is the UCM6100's IP address. Port 8089 on UCM6100 is used for HTTP server/web UI access. This setting will block host on 192.168.40.131 to access UCM6100 port 8089 using TCP connection.

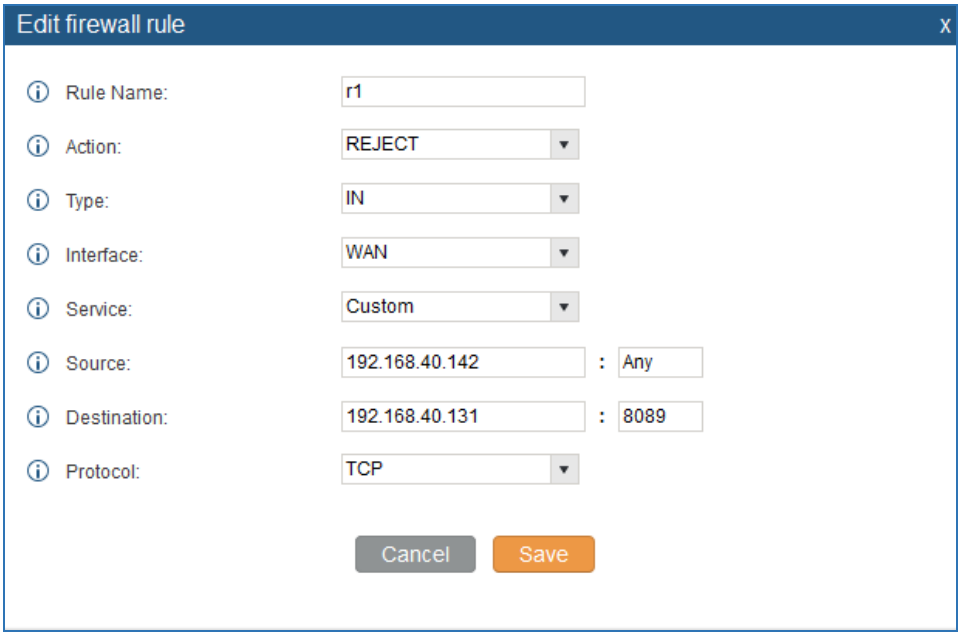


Figure 9: Firewall Rule Custom Configuration

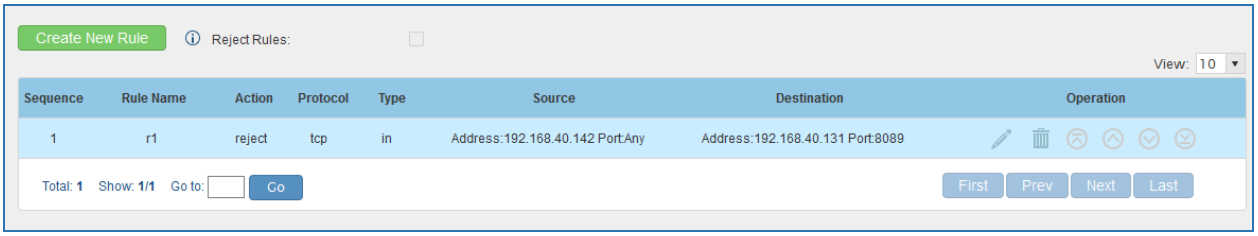


Figure 10: Static Defense Blocking Host 192.168.40.142 Using TCP Connection

After saving and applying the change, host 192.168.40.142 will not be able to access UCM6100 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
```

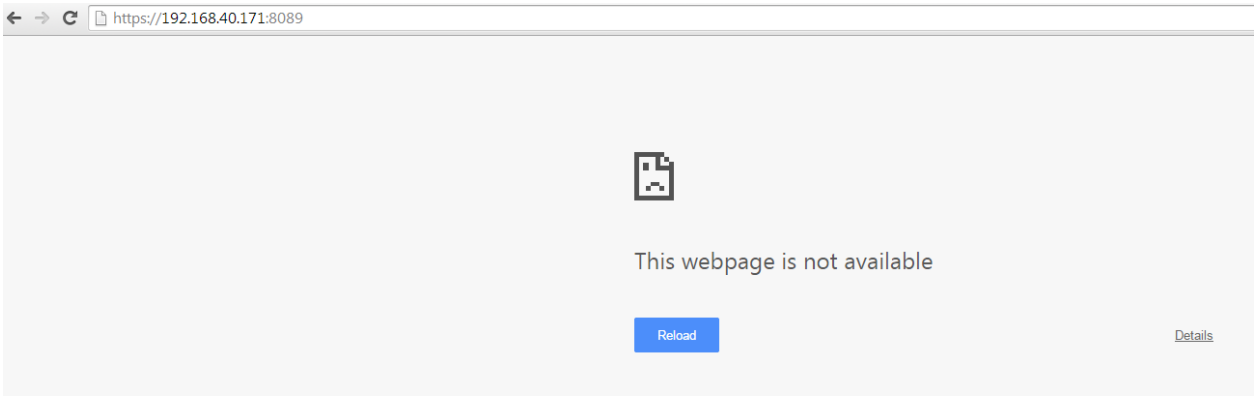


Figure 11: Host blocked by UCM6100

STATIC DEFENSE EXAMPLE: BLOCKING SSH CONNECTION TO UCM6100

The UCM6100 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 UCM6100 is deployed for security purpose. This can be done using static defense.

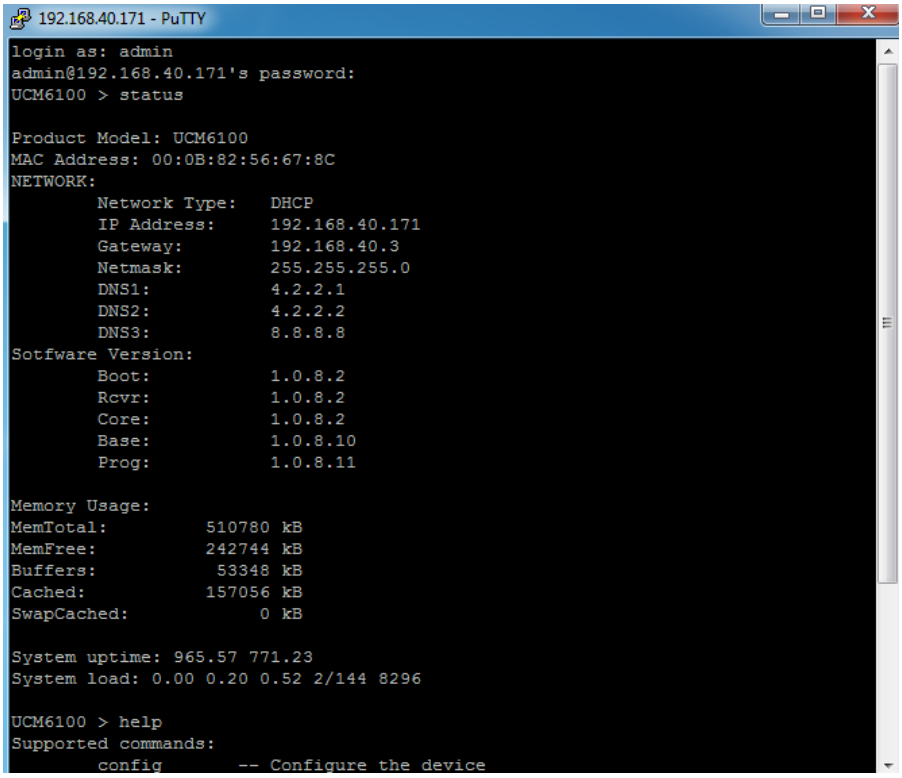


Figure 12: UCM6100 SSH Access

Configuration steps:

1. In UCM6100 web UI->Settings->Firewall->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 UCM6102).
   Service: SSH.

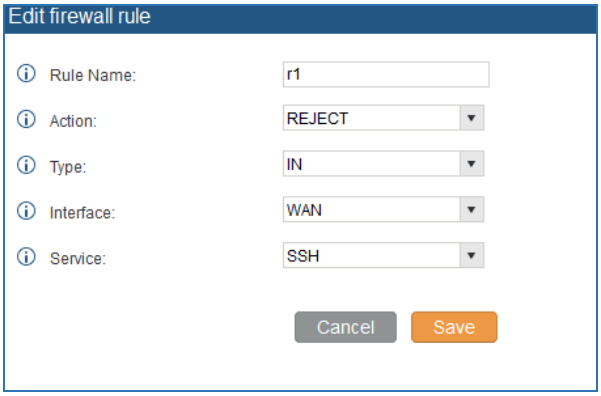


Figure 13: Block SSH Connection

3. Save and apply changes.

Now SSH connection to the UCM6100 will not be allowed anymore from any host.

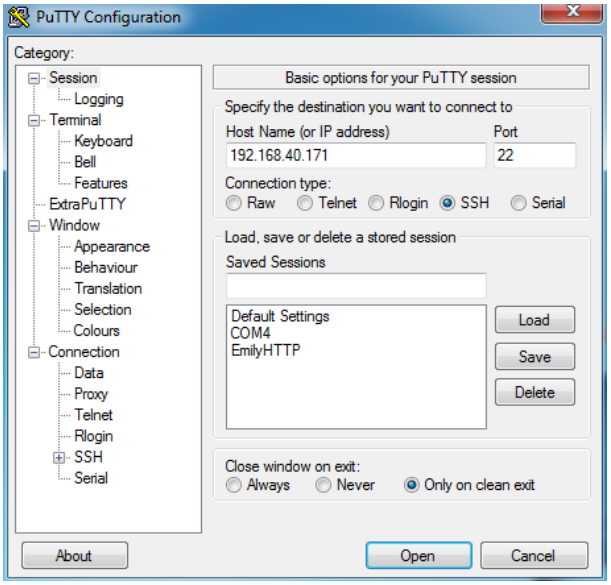


Figure 14: Putty Setup for SSH Connection

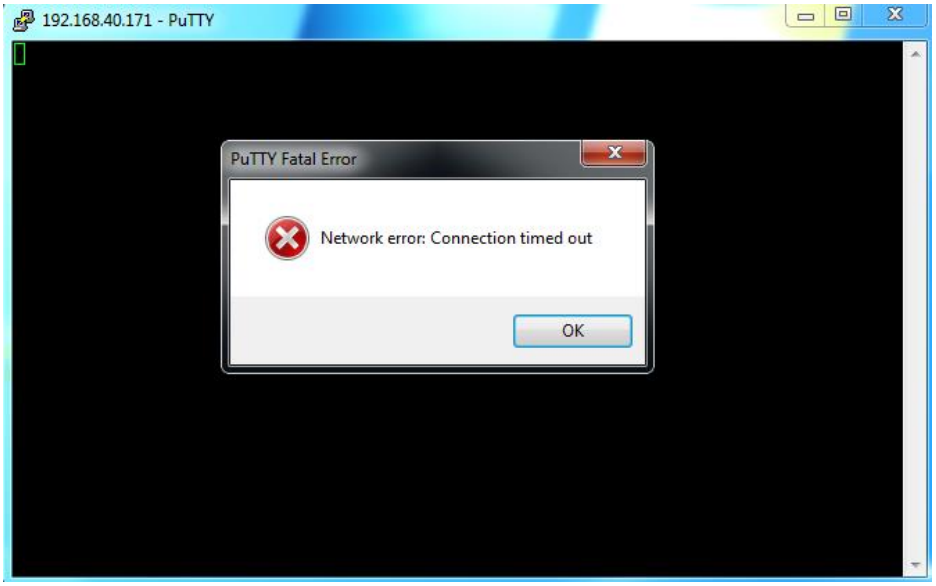


Figure 15: SSH Connection Blocked by UCM6100

DYNAMIC DEFENSE

Dynamic defense is supported on UCM6102 and UCM6510 when LAN mode is set to “Route”. It can be configured from Web UI->Settings->Firewall->Dynamic Defense. Once enabled, it will try to blacklist massive connection attempts or brute force attacks made by individual host.

The UCM6100 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 UCM6100 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->Settings->Firewall->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 UCM6100 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 UCM61xx web UI->Firewall->Fail2Ban. By default Fail2Ban is disabled

(see figure below).

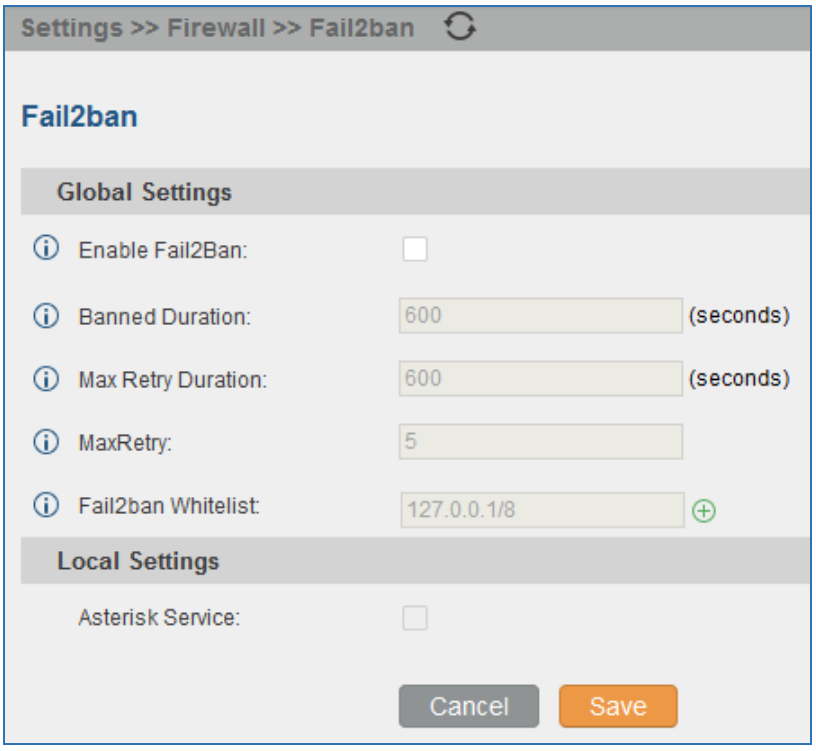


Figure 16: Fail2Ban Default Configuration

Enable Fail2Ban: Check it to enable Fail2Ban on the UCM6100.

Banned Duration: This specifies the amount of time the IP address will be blocked by UCM6100. 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 UCM6100. 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 UCM6100 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.

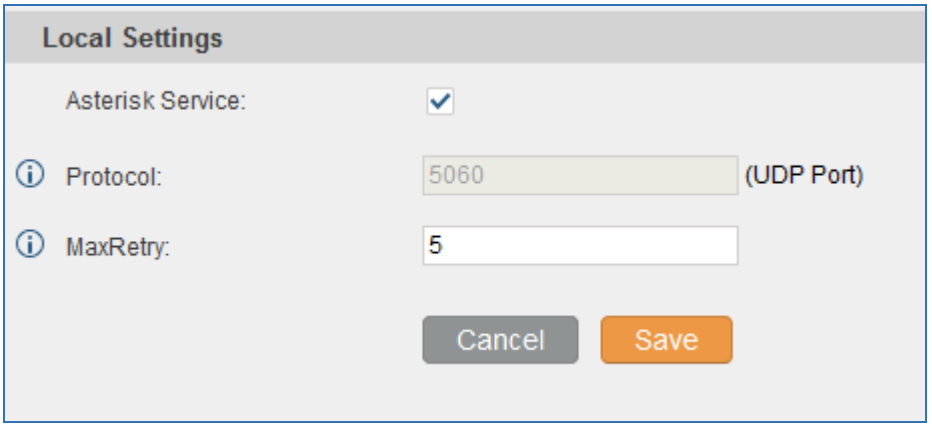


Figure 17: Asterisk Service Fail2Ban setting

If Fail2Ban is enabled under “Global Settings”, user must select “Asterisk Service” under “Local Settings” in order for it to take effect. Currently only 5060 (UCP Port) is supported for “Protocol”. 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.

AMI

Asterisk Manager Interface (AMI) is supported on UCM6100 with restricted access. The documentation can be found in the following link:

http://www.grandstream.com/products/ucm_series/ucm61xx/documents/ucm6100_ami_guide.pdf

Please do not enable AMI on the UCM6100 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 UCM6100 system. Please be cautious when enabling AMI access on the UCM6100 and restrict the permission granted to the AMI user.