Grandstream Networks, Inc.

UCM6XXX

Asterisk Manager Interface (AMI) Guide
# Table of Contents

INTRODUCTION .................................................................................................................. 3  
CREATING NEW AMI USER ............................................................................................... 4  
CONFIGURING AMI PORTS ................................................................................................. 6  
ESTABLISHING CONNECTION AND USER AUTHENTICATION ........................................ 8  
EXAMPLES .......................................................................................................................... 12

# Table of Figures

Figure 1: Web UI → Internal Options → AMI ...................................................................... 4  
Figure 2: Create New AMI User Dialog ............................................................................. 4  
Figure 3: AMI User Created .............................................................................................. 5  
Figure 4: AMI Settings ...................................................................................................... 6  
Figure 5: AMI Settings Dialog .......................................................................................... 6  
Figure 6: Telnet Settings in PuTTY .................................................................................... 8  
Figure 7: Telnet Connection Using PuTTY ......................................................................... 9  
Figure 8: Telnet Connection to AMI Using TCP ................................................................. 9  
Figure 9: Telnet Connection to AMI Using TLS ................................................................. 9  
Figure 10: User Authentication Successful ......................................................................... 10  
Figure 11: AMI Command Example .................................................................................. 11  
Figure 12: Example 1 - Originate Internal Call Ext 1000 to Ext 1001 ................................. 12  
Figure 13: Example 1 - Ext 1001 Ringing ......................................................................... 12  
Figure 14: Example 2 - Originate External Call ................................................................. 13  
Figure 15: Example 3 - Channel Hangup ......................................................................... 13  
Figure 16: Example 4 - Queue Status .............................................................................. 14  
Figure 17: GSAgents Command ....................................................................................... 15  
Figure 18: PJSIPShowEndpoints Command ..................................................................... 16  
Figure 19: PJSIPShowEndpoint Command ....................................................................... 17

# Table of Tables

Table 1: AMI User Privilege ............................................................................................... 5  
Table 2: AMI Settings Parameters .................................................................................... 6
INTRODUCTION

Asterisk Manager Interface (AMI) allows a client program to connect to an Asterisk instance and issue commands or read events over a TCP/IP stream. This is particularly useful when the integrators try to track the state of a telephony client inside Asterisk.

A simple “key: value” command line-based interface is utilized for communication between the connecting client and the Asterisk PBX. Lines are terminated by using CR/LF. In this document, we will use the term "packet" to describe a set of "key: value" lines that are terminated by an extra CR/LF.

Some useful Asterisk Manager Interface information can be found in the following links:

http://www.voip-info.org/wiki/view/Asterisk+manager+API

The UCM6XXX provides restricted AMI access for users. In order to connect to Asterisk Manager Interface on UCM6XXX, please follow the steps below.

1. Create new AMI user.
2. Configure AMI ports for connection.
3. Establish connection and authenticate the user.

This document introduces each step and necessary configurations in the following sections.

Note: UCM6XXX series include UCM6100 series (UCM6102, UCM6104, UCM6108 and UCM6116), UCM6200 series (UCM6202, UCM6204 and UCM6208) and UCM6510.

⚠️ Warning:

Please do not enable AMI on the UCM6XXX 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 UCM6XXX system. Please be cautious when enabling AMI access on the UCM6XXX and restrict the permission granted to the AMI user. By using AMI on UCM6XXX you agree you understand and acknowledge the risks associated with this.
CREATING NEW AMI USER

1. Log in the UCM6XXX web UI and navigate to **Value-added features → AMI**.
2. Click on “Create New AMI User”.

![Create New AMI User Dialog](image)

3. A new dialog “Create New AMI User” will be prompted.

4. Configure the following parameters in the “Create New AMI User” dialog:

   - **Username**
     Configure a name for new AMI user. The username needs to be at least 8 characters. For example, ucmamiuser1.

   - **Password**
     Configure a password for this user to connect to AMI for authentication purpose. The password has the following requirement:
     - at least 6 characters
     - must contain numeric digit
     - at least one lowercase alphabet, or one uppercase alphabet, or one special character

   - **Permitted IP(s)**
     Configure an IP address Access Control List (ACL) for addresses that should be allowed to authenticate
as the AMI user. **If not set, all IPs will be denied.** The format is IP/subnet. For example, 192.168.40.144/255.255.255.255.

- **Privilege**
  Configure the privilege for the AMI user. Please see options and definitions in below table.

<table>
<thead>
<tr>
<th>Privilege Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>This provides all privilege options to user.</td>
</tr>
<tr>
<td>Originate</td>
<td>Write-only. It provides permission to originate new calls.</td>
</tr>
<tr>
<td>Call</td>
<td>It provides permission to access information about channels and ability to configure in a running channel.</td>
</tr>
<tr>
<td>CDR</td>
<td>Read-only. This provides permission to obtain output of cdr-manager, if loaded.</td>
</tr>
<tr>
<td>Agent</td>
<td>This provides permission to access call queue information and agents’ information. It also provides ability to add members to a call queue.</td>
</tr>
<tr>
<td>CC</td>
<td>Read-only. This provides permission to receive Call Completion events.</td>
</tr>
<tr>
<td>DTMF</td>
<td>Read-only. This provides permission to receive DTMF events.</td>
</tr>
<tr>
<td>Dialplan</td>
<td>Read-only. This provides permission to receive NewExten and VarSet events.</td>
</tr>
<tr>
<td>Reporting</td>
<td>This provides ability to obtain statistics and status information from the system.</td>
</tr>
<tr>
<td>User Events</td>
<td>This provides permission to send and receive UserEvent.</td>
</tr>
<tr>
<td>Security Events</td>
<td>Read-only. It provides ability to read security events.</td>
</tr>
<tr>
<td>Special Command</td>
<td>This provides permission to “command” privilege to show information about queue agents, individual and all SIP endpoints.</td>
</tr>
</tbody>
</table>

5. Click on **Save** and then **Apply Changes**.

**Figure 3: AMI User Created**

Now the AMI user is successfully created. After creating the AMI user, it can be edited by clicking on 🔄 icon or deleted by clicking on 🗑️ icon.
CONFIGURING AMI PORTS

1. In UCM6XXX web UI→Value-added features→AMI page, click on “AMI Settings”.

![AMI Settings](image)

Figure 4: AMI Settings

2. A new dialog “AMI Settings” will be prompted.

![AMI Settings Dialog](image)

Figure 5: AMI Settings Dialog

3. Configure the following parameters in “AMI Settings” dialog. Users can connect AMI using TCP or TLS. If using TLS, please set “TLS Enable” to “Yes”.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI Port</td>
<td>Configures the port number to listen to for AMI connection.</td>
</tr>
<tr>
<td></td>
<td>The default setting is 7777.</td>
</tr>
<tr>
<td>TLS Enable</td>
<td>Enables listening for AMI connections using TLS.</td>
</tr>
<tr>
<td></td>
<td>The default setting is No.</td>
</tr>
<tr>
<td>TLS Port</td>
<td>Configures the port to listen to for TLS-based AMI connection.</td>
</tr>
<tr>
<td></td>
<td>The default setting is 5039.</td>
</tr>
</tbody>
</table>

Table 2: AMI Settings Parameters
<table>
<thead>
<tr>
<th><strong>Write Timeout</strong></th>
<th>Sets the timeout when writing data to the AMI connection for this user. This option is specified in milliseconds. The default value is 100.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLS Bind Address</strong></td>
<td>Configures the address to listen to for TLS-based AMI connections. The default setting is 0.0.0.0, which means all addresses.</td>
</tr>
<tr>
<td><strong>Timestamp Events</strong></td>
<td>Add a Unix epoch timestamp to events.</td>
</tr>
<tr>
<td><strong>TLS Private Key</strong></td>
<td>Upload TLS private key for TLS-based AMI connection. The size of the key file must be under 2 MB. After uploading, the file will be automatically renamed to “ami_private.pem”.</td>
</tr>
<tr>
<td><strong>TLS Cert</strong></td>
<td>Upload the TLS cert for TLS-based AMI connection. It contains private key for the client and signed certificate for the server. The size of the certificate must be under 2MB. After uploading, the file will be automatically renamed to “ami_certificate.pem”.</td>
</tr>
</tbody>
</table>

4. Click on “Save” and then “Apply Changes” to save the AMI settings.
ESTABLISHING CONNECTION AND USER AUTHENTICATION

1. To connect AMI using TCP, simply use Telnet to connect to UCM6XXX’s IP address with AMI port.

   - If using command line, users can type in:  
     
     \[ \text{telnet 192.168.40.237 7777} \]

   - If using PuTTY, users might need change the Telnet setting “Telnet Negotiation Mode” to “Passive” first. Then initiate Telnet connection to AMI from Putty.

   ![PuTTY Configuration](image)

   Figure 6: Telnet Settings in PuTTY
2. After initiating connection, users shall see prompt like below, meaning connection is established.

```
Asterisk Call Manager/2.7.0
```

![Figure 8: Telnet Connection to AMI Using TCP](image8.png)

3. To connect AMI using TLS, use the following format to connect the TLS port in command line:

```
root@ubuntu:~# telnet -z ssl -z cert=certificate.pem -z key=private.pem 172.16.0.73 5039
```

```
Trying 172.16.0.73...
SSL: Server has a self-signed certificate
SSL: unknown issuer: /C=US/ST=TX/L=Plano/O=Grandstream/OU=Dev/CN=Philip Neuman/emailAddress=pneuman@grandstream.com
Connected to 172.16.0.73.
Escape character is '^]'.
```

![Figure 9: Telnet Connection to AMI Using TLS](image9.png)

The IP address is the UCM6XXX IP and 5039 is the TLS port.

4. After the connection is established, the system will wait for user’s input. By default, if there is no input in 30 seconds, the system will disconnect automatically.
5. To log in and get authenticated, manually enter all the text below:

```plaintext
action: login
username: <ucmamiuser1>
secret: <test123>
```

Tap on ENTER and users should see response like below. Sometimes if there is no response after ENTER, please tap on ENTER again.

![User Authentication Successful](image.png)

**Figure 10: User Authentication Successful**

**Note:** Users must log in and get authenticated before using other commands.

6. To view all executable AMI commands, enter text below:

```plaintext
action: listcommands
```

Tap on ENTER. Users will see the following output. (Sometimes if there is no response after ENTER, please tap on ENTER again.)
Figure 11: AMI Command Example
EXAMPLES

There are mainly 3 types of AMI packets:

- **Action**: packets sent by client to Asterisk to request to perform a particular action. There are a limited number of actions for the client to use and each of them is decided by the module in Asterisk server. Only one action can be performed each time and the action packet contains the action name and parameters.

- **Response**: response by Asterisk to the client action.

- **Event**: information about the events of Asterisk core or expansion modules.

**Note**: Please make sure the AMI user is logged in and authenticated first

**Example 1: Originates an internal call**

![Figure 12: Example 1 - Originate Internal Call Ext 1000 to Ext 1001](image)

![Figure 13: Example 1 - Ext 1001 Ringing](image)
Example 2: Originate an external call via trunk

![Example 2 - Originate External Call](image)

Example 3: Channel hang-up

*Note:* This command will hang up active call.

![Example 3 - Channel Hangup](image)
Example 4: Query the status of queue

Figure 16: Example 4 - Queue Status
Example 5: Query the status of agents in queues

```
Polling: GSAgents
Response: Success
EventList: start
Message: Agents status will follow

Event: GsAgent
Agent: PJSIP/1005
QueueName: Support
Queue: 6500
Location: PJSIP/1005
Membership: static
Penalty: 0
CallsTaken: 0
LastCall: 0
Status: 1
LoginTime: 0
callsAbandon: 1
TalkTime: 0
CallerChannel: Paused: 0

Event: GsAgent
Agent: PJSIP/1000
QueueName: Support
Queue: 6500
Location: PJSIP/1000
Membership: static
Penalty: 0
CallsTaken: 3
LastCall: 1534757230
Status: 1
LoginTime: 0
callsAbandon: 4
TalkTime: 175
CallerChannel: PJSIP/1000-00000014
Paused: 0

Event: GsAgent
Agent: PJSIP/1001
QueueName: Staff
Queue: 6501
Location: PJSIP/1001
Membership: static
Penalty: 0
CallsTaken: 0
LastCall: 0
Status: 5
LoginTime: 0
callsAbandon: 0
TalkTime: 0
CallerChannel: Paused: 0

Event: GsAgent
Agent: PJSIP/1005
```

Figure 17: GSAgents Command
Example 6: PJSIPShowEndpoints query to get extensions and trunks status

Figure 18: PJSIPShowEndpoints Command
Example 6: PJSIPShowEndpoint query to get specific endpoint details

Figure 19: PJSIPShowEndpoint Command

* Asterisk is a Registered Trademark of Digium, Inc.