Grandstream Networks, Inc.

UCM6100 Asterisk Manager Interface (AMI) Guide

Index

Table of Contents

Table of Figures

Table of Tables

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**" line-based protocol 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
https://wiki.asterisk.org/wiki/pages/viewpage.action?pageId=4817239

The UCM6100 provides restricted AMI access for users. In order to connect to Asterisk Manager Interface on UCM6100, 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.

⚠ **Warning:**

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. By using AMI on UCM6100 you agree you understand and acknowledge the risks associated with this.

---

1. CREATING NEW AMI USER

1.1. Log in the UCM6100 web UI and navigate to **PBX**->**Internal Options**->**AMI**.

1.2. Click on “Create New AMI User”.

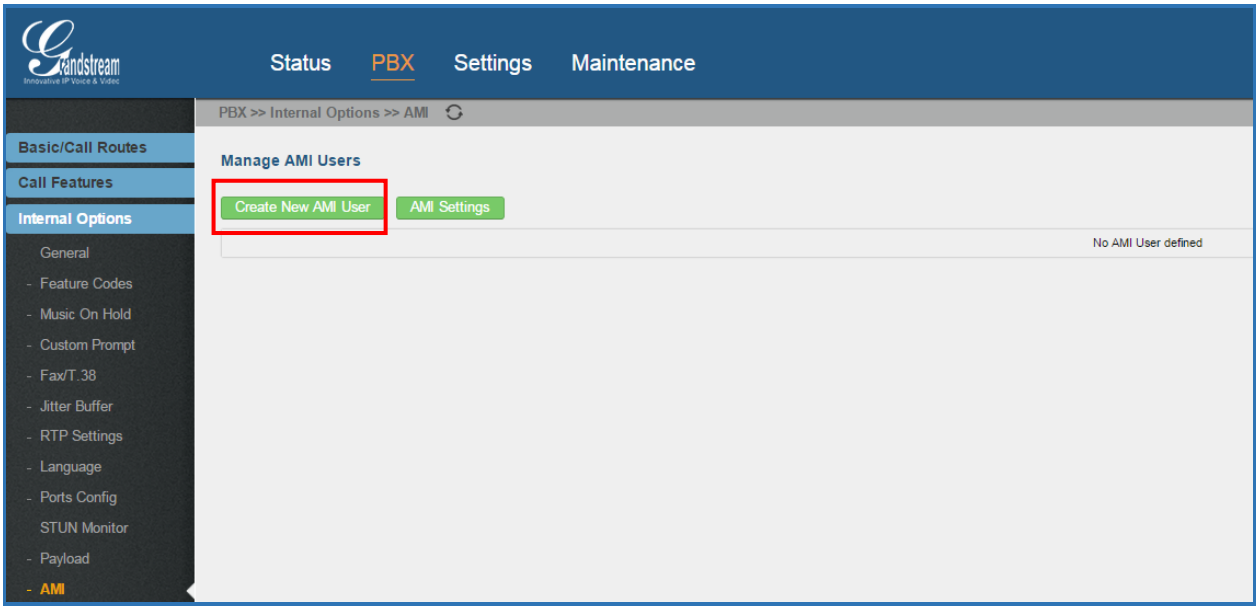

Figure 1: Web UI->Internal Options->AMI

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

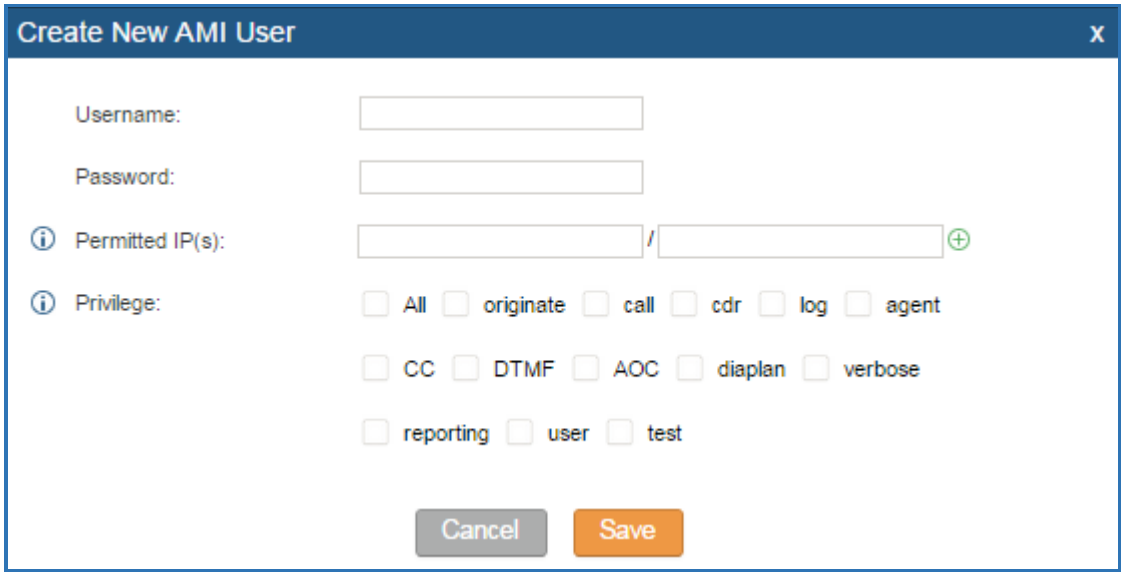

Figure 2: Create New AMI User Dialog

1.4. 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 1: AMI User Privilege

Privilege Option	Definition
originate	It provides permission to originate new calls.
call	It provides permission to access information about channels and ability to configure in a running channel.
cdr	Read-only. This provides permission to obtain output of cdr-manager, if loaded.
log	Read-only. This provides permission to obtain logging information.
agent	This provides permission to access call queue information and agents' information. It also provides ability to add members to a call queue.
CC	Read-only. This provides permission to receive Call Completion events.
DTMF	Read-only. This provides permission to receive DTMF events.
AOC	This provides permission to send Advice Of Charge messages and receive Advice Of Change events.
dialplan	Read-only. This provides permission to receive NewExten and VarSet events.
verbose	Read-only. This provides permission to obtain verbose information.
reporting	This provides ability to obtain system information.
user	This provides permission to send and receive UserEvent.
test	This provides ability to read TestEvent notifications sent to the Asterisk Test Suite. Please note this is only enabled when the TEST-FRAMEWORK complier flag is defined.

1.5. 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.

2. CONFIGURING AMI PORTS

2.1. In UCM6100 web UI->**PBX**->**Internal Options**->**AMI** page, click on “AMI Settings”.

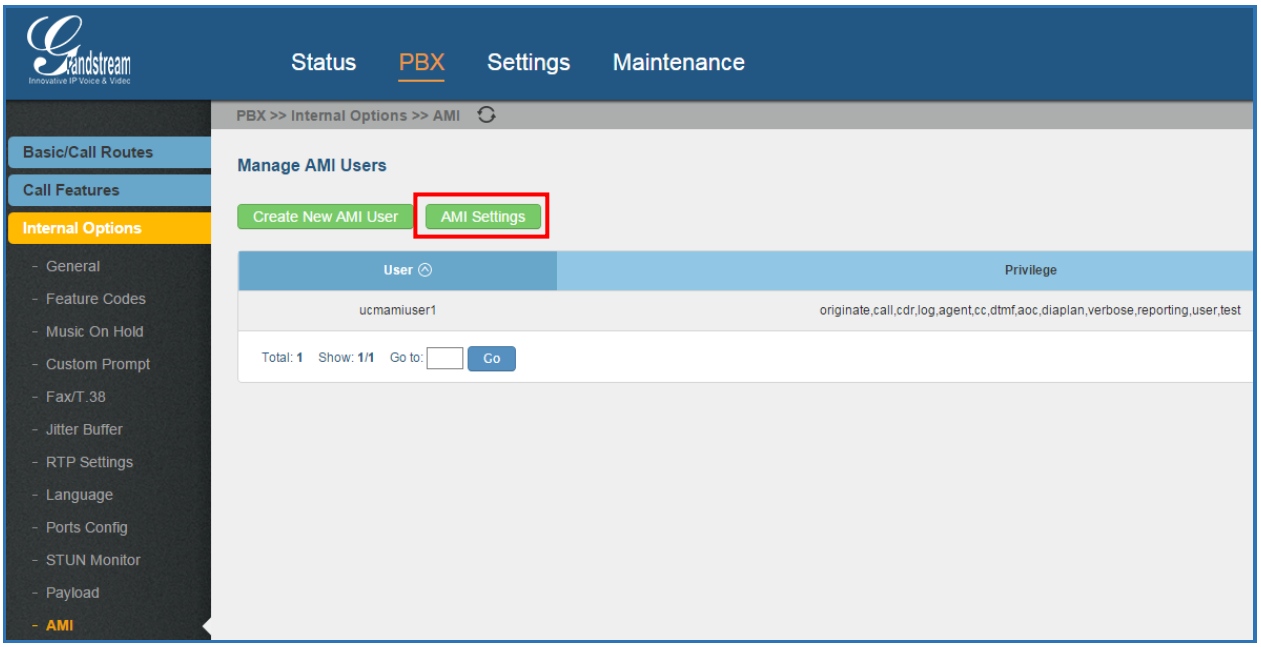

Figure 4: AMI Settings

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

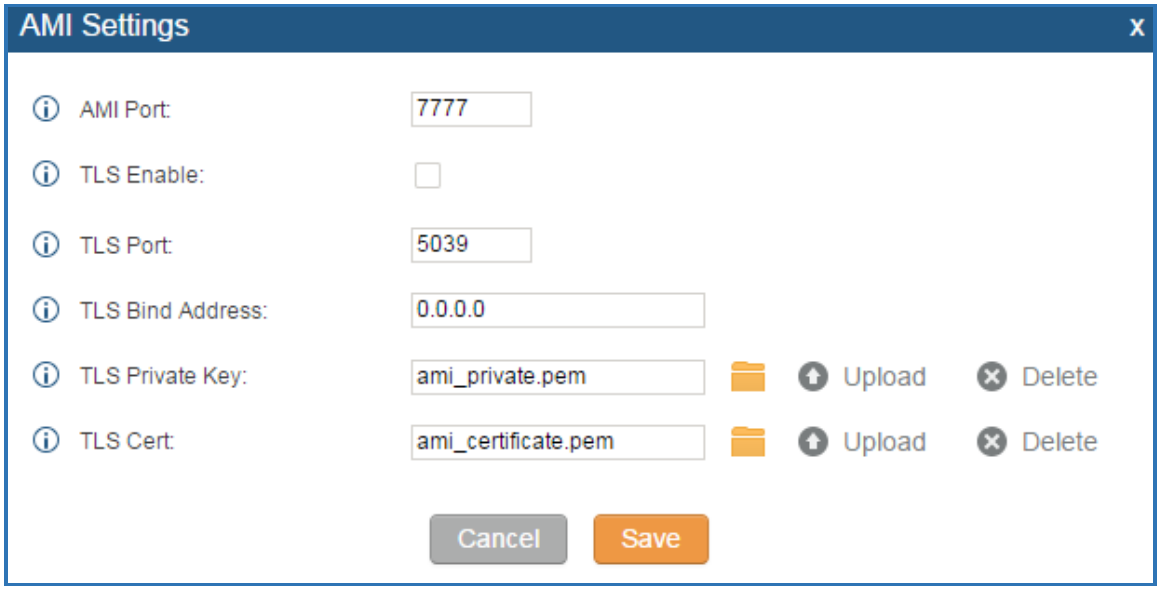

Figure 5: AMI Settings Dialog

2.3. 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 2: AMI Settings Parameters

Parameter	Definition
AMI Port	Configures the port number to listen to for AMI connection. The default setting is 7777.
TLS Enable	Enables listening for AMI connections using TLS. The default setting is No.
TLS Port	Configures the port to listen to for TLS-based AMI connection. The default setting is 5039.
TLS Bind Address	Configures the address to listen to for TLS-based AMI connections. The default setting is 0.0.0.0, which mean all addresses.
TLS Private Key	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”.
TLS Cert	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”.

2.4. Click on “Save” and then “Apply Changes” to save the AMI settings.

3. ESTABLISHING CONNECTION AND USER AUTHENTICATION

3.1. To connect AMI using TCP, simply use Telnet to connect to UCM6100's IP address with AMI port.

- If using command line, users can type in:
  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.

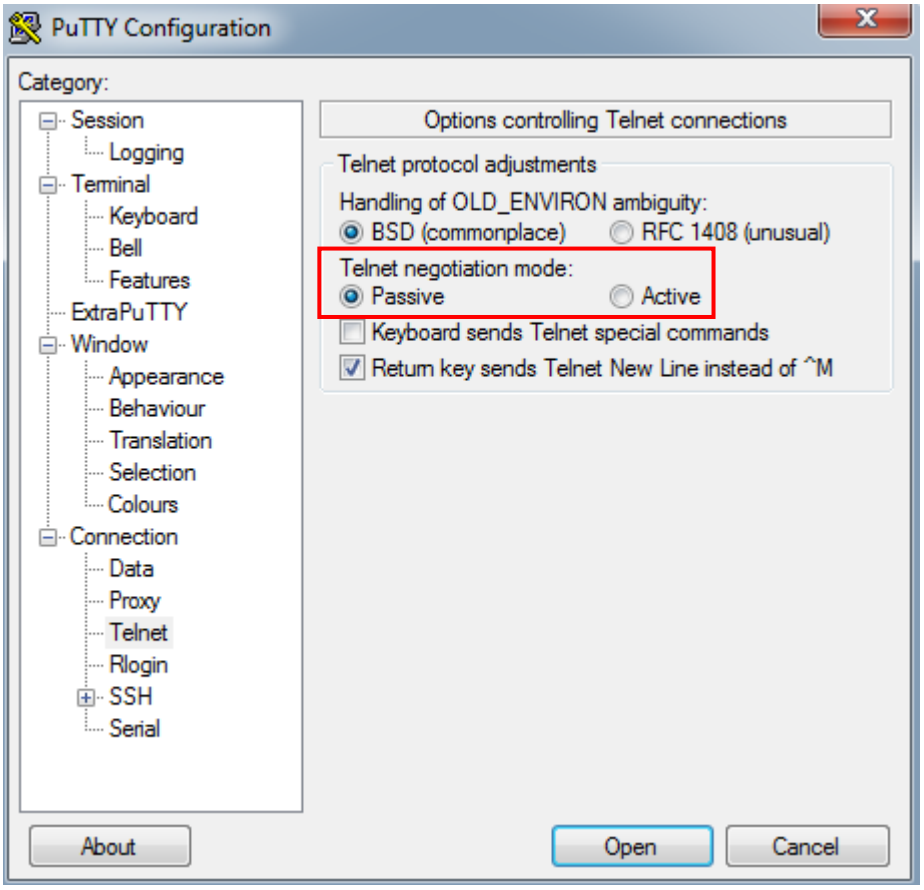

Figure 6: Telnet Settings in PuTTY

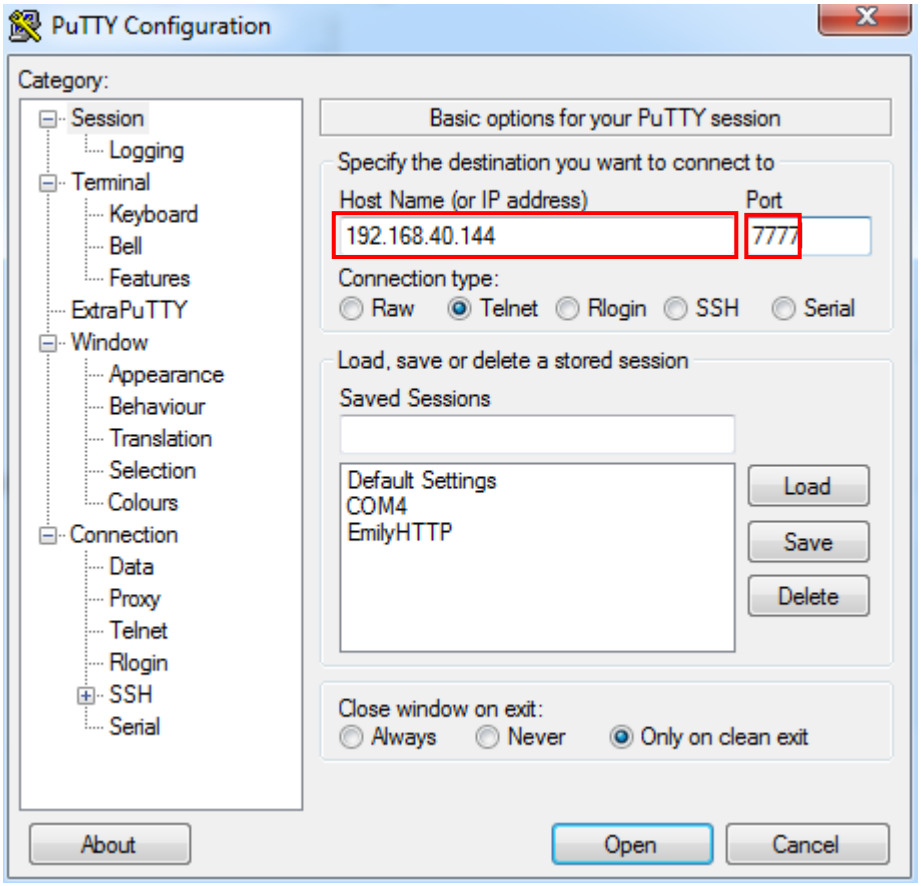

Figure 7: Telnet Connection Using PuTTY

3.2. After initiating connection, users shall see prompt like below, meaning connection is established.

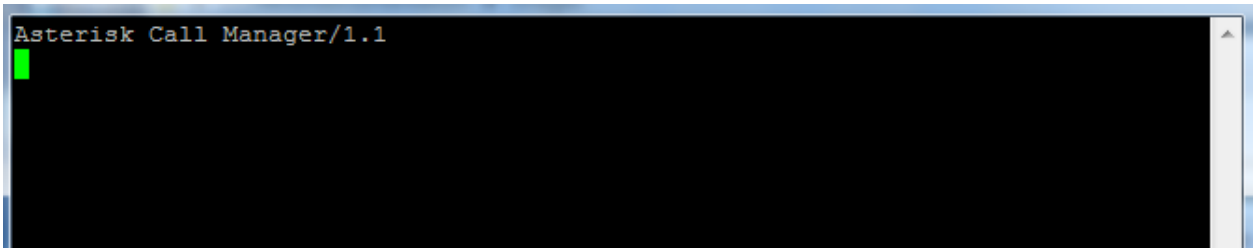

Figure 8: Telnet Connection to AMI Using TCP

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

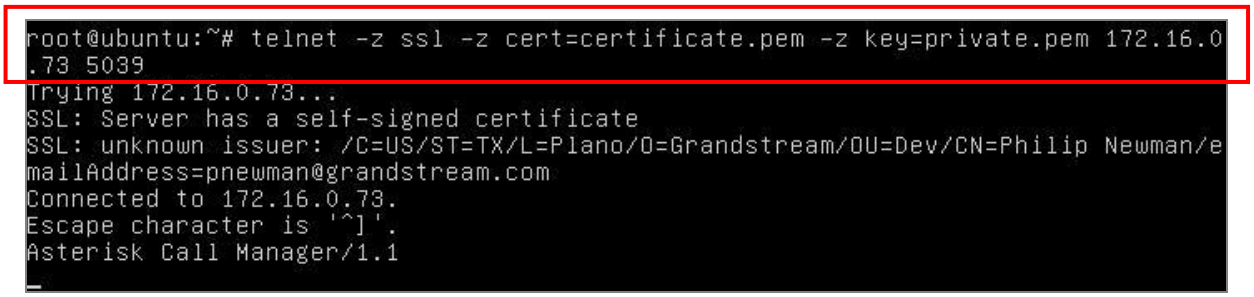

Figure 9: Telnet Connection to AMI Using TLS

The IP address is the UCM6100 IP and 5039 is the TLS port.

3.4. 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.

3.5. To log in and get authenticated, manually enter all the text below:

action: login
username: ucmamiuser1
secret: admin1234

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

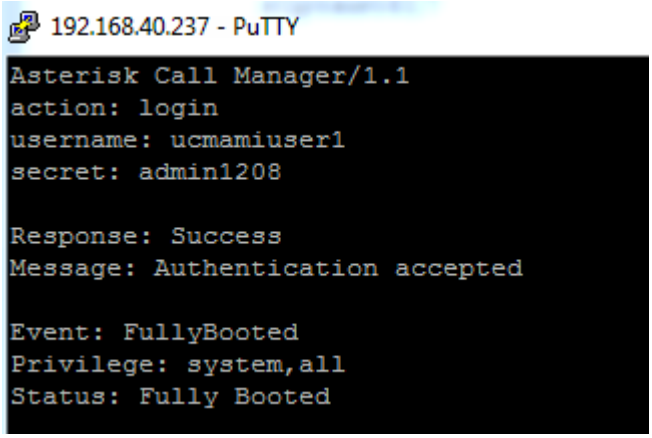

Figure 10: User Authentication Successful

3.6. To view all executable AMI command, enter text below:
action: listcommands

Tap on ENTER. Users will see the following output. The highlighted command is corresponding to

the options selected in “Privilege” setting. (Sometimes if there is no response after ENTER, please tap on ENTER again.)

```
action: listcommands

Response: Success
WaitEvent: Wait for an event to occur.  (Priv: <none>)
QueueReset: Reset queue statistics.  (Priv: <none>)
QueueReload: Reload a queue, queues, or any sub-section of a queue or queues.  (
Priv: <none>)
QueueRule: Queue Rules.  (Priv: <none>)
QueueSummary: Show queue summary.  (Priv: <none>)
QueueStatus: Show queue status.  (Priv: <none>)
Queues: Queues.  (Priv: <none>)
MixMonitorMute: Mute / unMute a Mixmonitor recording.  (Priv: <none>)
AnalogChanlists:  (Priv: <none>)
DAHDIRestart: Fully Restart DAHDI channels (terminates calls).  (Priv: <none>)
DAHDIShowChannels: Show status of DAHDI channels.  (Priv: <none>)
DAHDIDNDoff: Toggle DAHDI channel Do Not Disturb status OFF.  (Priv: <none>)
DAHDIDNDon: Toggle DAHDI channel Do Not Disturb status ON.  (Priv: <none>)
DAHDIDialOffhook: Dial over DAHDI channel while offhook.  (Priv: <none>)
DAHDIHangup: Hangup DAHDI Channel.  (Priv: <none>)
DAHDITransfer: Transfer DAHDI Channel.  (Priv: <none>)
ParkedCalls: List parked calls.  (Priv: <none>)
ListCommands: List available manager commands.  (Priv: <none>)
Originate: Originate a call.  (Priv: originate,all)
Ping: Keepalive command.  (Priv: <none>)
Challenge: Generate Challenge for MD5 Auth.  (Priv: <none>)
Login: Login Manager.  (Priv: <none>)
Logoff: Logoff Manager.  (Priv: <none>)
Events: Control Event Flow.  (Priv: <none>)
DataGet: Retrieve the data api tree.  (Priv: <none>)
```

Figure 11: AMI Command Example

4. EXAMPLE

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.

Here are some examples output.

Example 1: Query the status of parked call

```
Event: ParkedCall
Parkinglot: default
Exten: 701
Channel: SIP/3005-00000000
From: SIP/3005-00000000
Timeout: 284
CallerIDNum: 3005
CallerIDName:
ConnectedLineNum:
ConnectedLineName:

Event: ParkedCallsComplete
Total: 1
```

Figure 12: Example 1 – Parked Call Status

Example 2: Query the status of queue

```
action: queues

Response: Success
EventList: start
Message: Queues list will follow

Event: QueueStatus
Queue: 6500
CallCount: 0
CallsComplete: 0
CallsAbandoned: 0
SeviceLevel: SL:0.0% within 0s

Event: QueueMemberStatus
Queue: 6500
Location: SIP/3003
MemberName: SIP/3003
Membership: static
Penalty: 0
CallsTaken: 0
LastCall: 0
Status: 5
Paused: 0
```

Figure 13: Example 2 – Queue Status

Example 3: Execute the command exceeding the privileges

```
action: hangup
channel: sip/3005-00000028

Response: Error
Message: Permission denied
```

Figure 14: Example 3 – Permission Denied After Query without Proper Privilege

Example 4: Log off and disconnect

```
action: logoff

Response: Goodbye
Message: Thanks for all the fish.
```

Figure 15: Example 4 – Log Off

Example 5: Log in authentication failure and disconnect.

```
Asterisk Call Manager/1.1
action: login
username: zhangjing1991
secret: jing1991

Response: Error
Message: Authentication failed
```

Figure 16: Example 5 – Authentication Failed

This document can be downloaded here:

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