FIBERME Communications LLC.

FCM630A - Asterisk Manager Interface (AMI) Guide

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 thestate 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

https://wiki.asterisk.org/wiki/pages/viewpage.action?pageId=4817239

The FCM630A provides restricted AMI access for users. In order to connect to Asterisk Manager Interface onFCM630A, please follow the steps below.

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

⚠ **Warning:**

Please do not enable AMI on the FCM630A 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 FCM630A system. Please be cautious when enabling AMI access on the FCM630A and restrict the permission granted to the AMI user. By using AMI on FCM630A you agree you understand and acknowledge the risks associated with this.

CREATING NEW AMI USER

1. Log in the FCM630A web UI and navigate to **Value-added features→AMI**.
2. Click on “Add”.

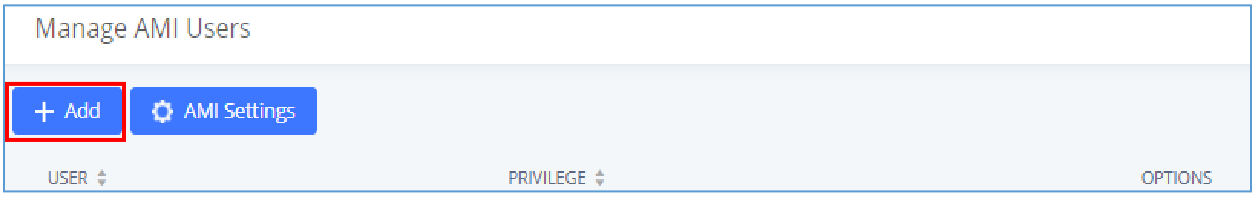
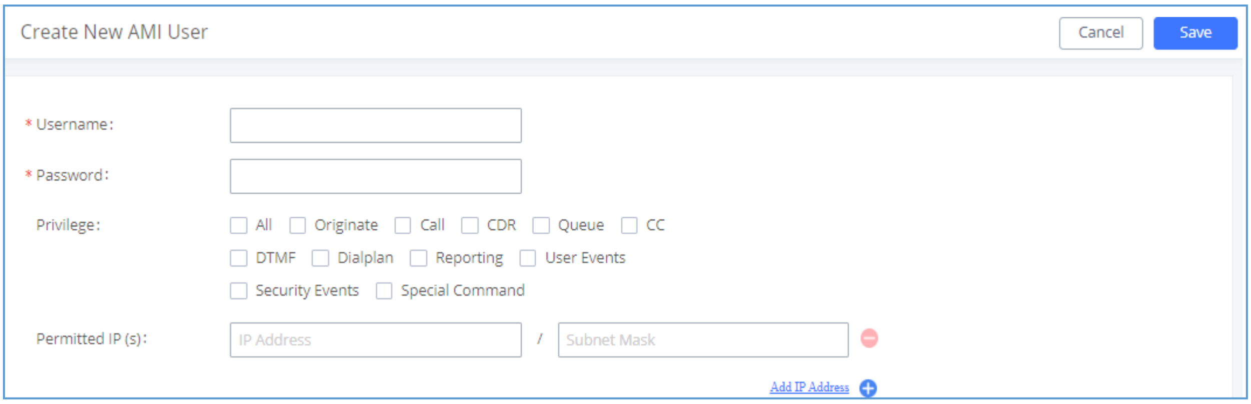


Figure 1: Web UI→Internal Options→AMI

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



Create New AMI User
Cancel
Save
* Username:
* Password:
Privilege:
□ All □ Originate □ Call □ CDR □ Queue □ CC
□ DTMF □ Dialplan □ Reporting □ User Events
□ Security Events □ Special Command
Permitted IP (s):
IP Address
/
Subnet Mask
Add IP Address

Figure 2: Create New AMI User Dialog

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, admin123

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

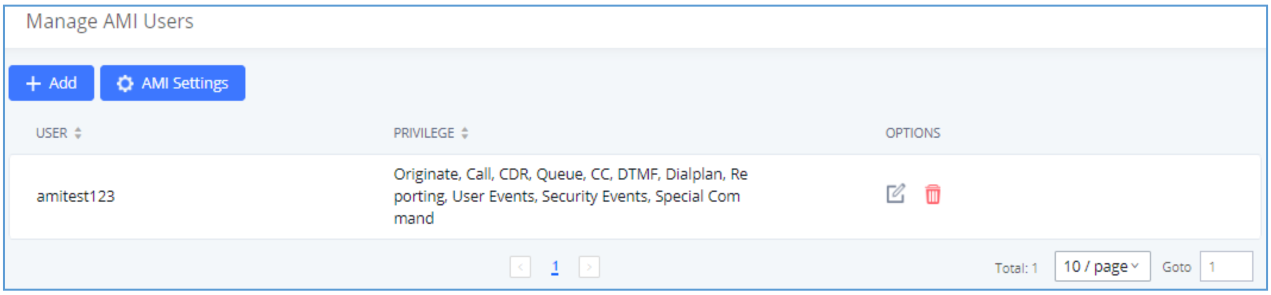
- **Permitted IP(s)**
  Configure an IP address Access Control List (ACL) for addresses that should be allowed to authenticate as the AMI user. If not set, all IPs will be denied. The format is IP/subnet. For example, 192.168.40.144/255.255.255.255.

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

Table 1: AMI User Privilege

Privilege Option	Definition
All	This provides all privilege options to user.
Originate	Write-only. 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.
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.
Dialplan	Read-only. This provides permission to receive NewExten and VarSet events.
Reporting	This provides ability to obtain statistics and status information from the system.
User Events	This provides permission to send and receive UserEvent.
Security Events	Read-only. It provides ability to read security events.
Special Command	This provides permission to "command" privilege to show information about queue agents, individual and all SIP endpoints.

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



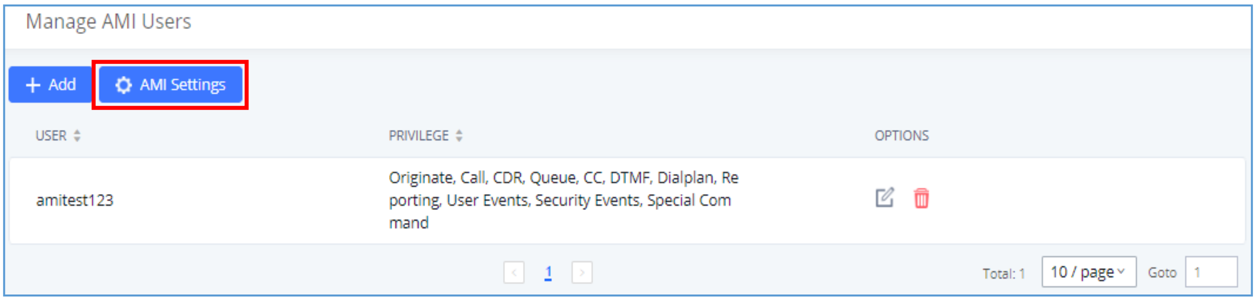
USER	PRIVILEGE	OPTIONS
amitest123	Originate, Call, CDR, Queue, CC, DTMF, Dialplan, Reporting, User Events, Security Events, Special Command	✎ 🗑

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

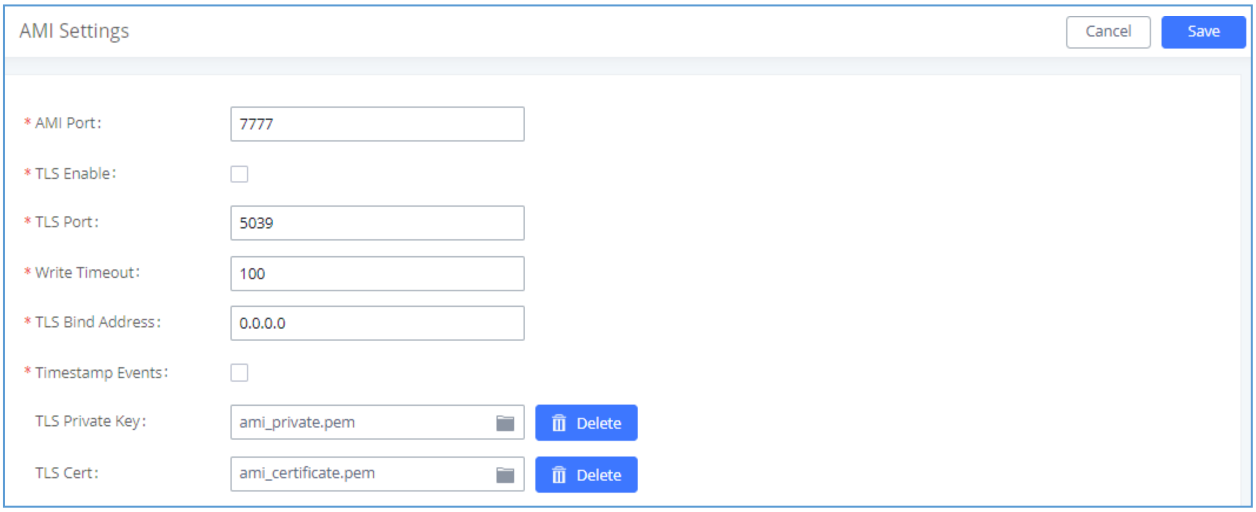
1. In FCM630A web UI→**Value-added features→AMI** page, click on “AMI Settings”.



USER	PRIVILEGE	OPTIONS
amitest123	Originate, Call, CDR, Queue, CC, DTMF, Dialplan, Reporting, User Events, Security Events, Special Command	

Figure 4: AMI Settings

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



* AMI Port: 7777

* TLS Enable: □

* TLS Port: 5039

* Write Timeout: 100

* TLS Bind Address: 0.0.0.0

* Timestamp Events: □

TLS Private Key: ami_private.pem

TLS Cert: ami_certificate.pem

Figure 5: AMI Settings Dialog

3. Configure the following parameters in “AMI Settings” dialog. Users can connect AMI using TCP orTLS. 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.

Write Timeout	Sets the timeout when writing data to the AMI connection for this user. This option is specified in milliseconds. The default value is 100.
TLS Bind Address	Configures the address to listen to for TLS-based AMI connections. The default setting is 0.0.0.0, which means all addresses.
Timestamp Events	Add a Unix epoch timestamp to events.
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”.

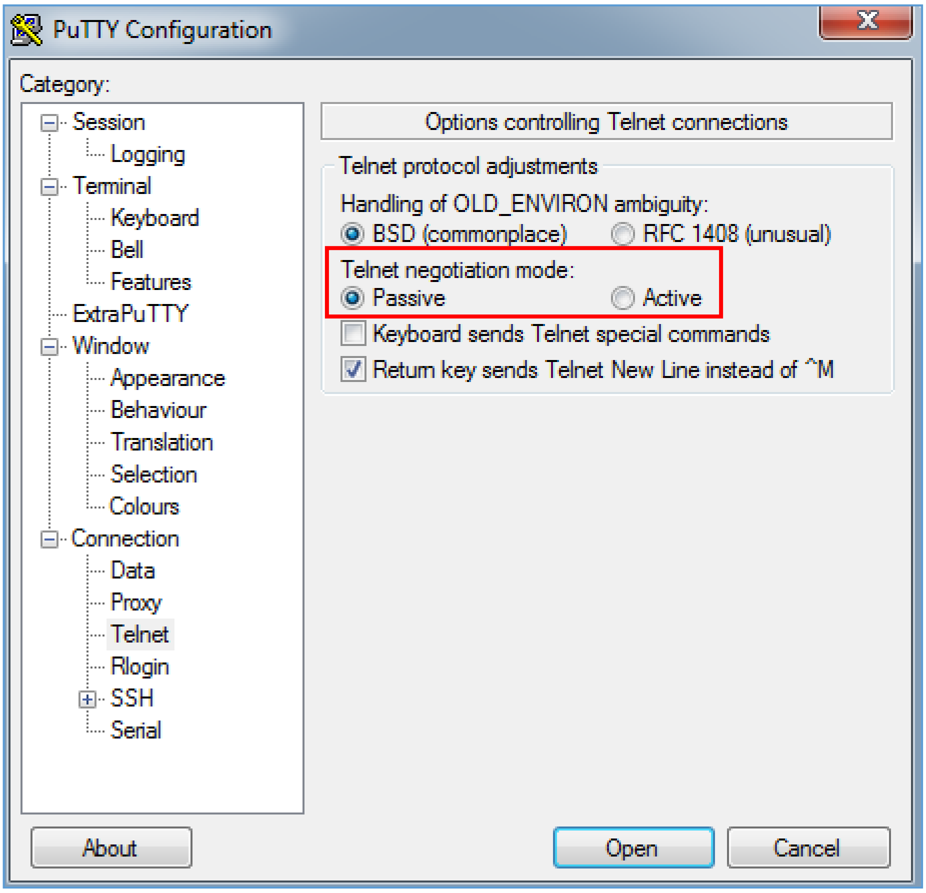
4. Click on “Save” and then “Apply Changes” to save the AMI settings.

ESTABLISHING CONNECTION AND USER AUTHENTICATION

1. To connect AMI using TCP, simply use Telnet to connect to FCM630A'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.



Options controlling Telnet connections

Telnet protocol adjustments

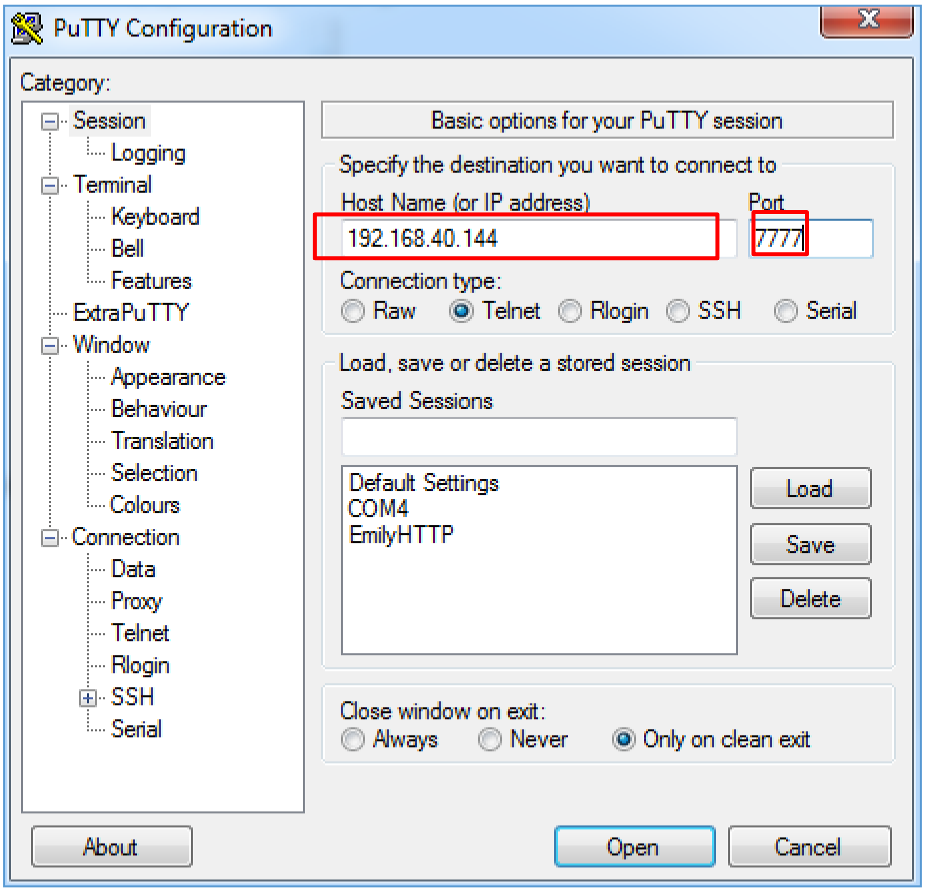
Handling of OLD_ENVIRON ambiguity:
● BSD (commonplace) ○ RFC 1408 (unusual)

Telnet negotiation mode:
● Passive ○ Active

□ Keyboard sends Telnet special commands

☑ Return key sends Telnet New Line instead of ^M

Figure 6: Telnet Settings in PuTTY



Host Name (or IP address): 192.168.40.144

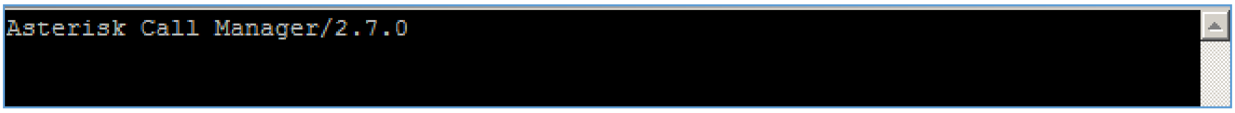
Port: 7777

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

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

Figure 7: Telnet Connection Using PuTTY

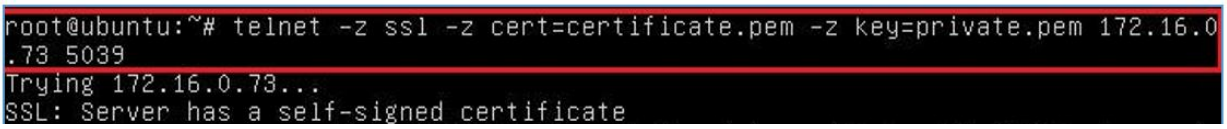
2. After initiating connection, users shall see prompt like below, meaning connection is established.



```
Asterisk Call Manager/2.7.0
```

Figure 8: Telnet Connection to AMI Using TCP

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
```

Figure 9: Telnet Connection to AMI Using TLS

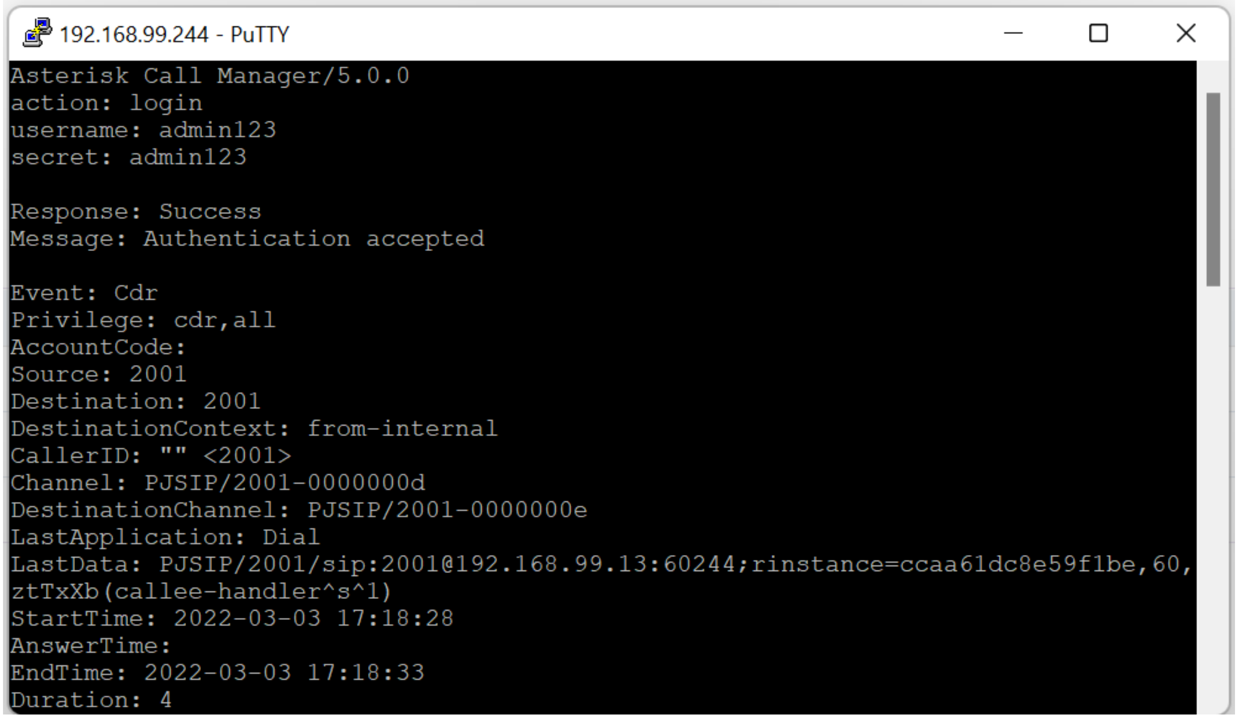
The IP address is the FCM630A IP and 5039 is the TLS port.

4. After the connection is established, the system will wait for user’s input. By default, if there is no inputin 30 seconds, the system will disconnect automatically.

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

action: login
username: <admin123>
secret: <admin123>

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



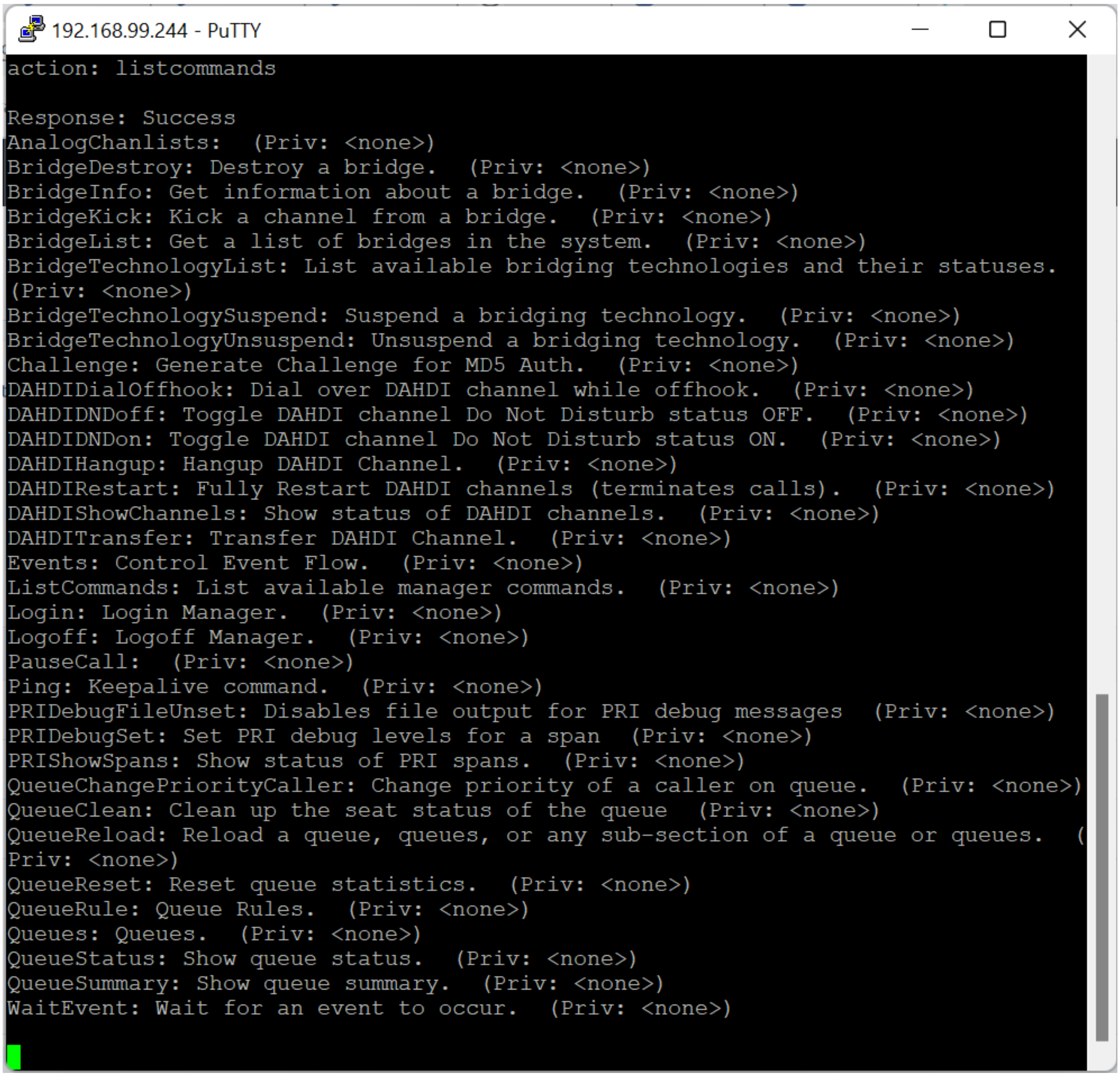
```
Asterisk Call Manager/5.0.0
action: login
username: admin123
secret: admin123

Response: Success
Message: Authentication accepted

Event: Cdr
Privilege: cdr,all
AccountCode:
Source: 2001
Destination: 2001
DestinationContext: from-internal
CallerID: "" <2001>
Channel: PJSIP/2001-0000000d
DestinationChannel: PJSIP/2001-0000000e
LastApplication: Dial
LastData: PJSIP/2001/sip:2001@192.168.99.13:60244;rinstance=ccaa61dc8e59f1be,60,
ztTxXb(callee-handler^s^1)
StartTime: 2022-03-03 17:18:28
AnswerTime:
EndTime: 2022-03-03 17:18:33
Duration: 4
```

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:
action:listcommands

Tap on ENTER. Users will see the following output. (Sometimes if there is no response after ENTER,please tap on ENTER again.)



```
action: listcommands

Response: Success
AnalogChanlists:  (Priv: <none>)
BridgeDestroy: Destroy a bridge.  (Priv: <none>)
BridgeInfo: Get information about a bridge.  (Priv: <none>)
BridgeKick: Kick a channel from a bridge.  (Priv: <none>)
BridgeList: Get a list of bridges in the system.  (Priv: <none>)
BridgeTechnologyList: List available bridging technologies and their statuses.
 (Priv: <none>)
BridgeTechnologySuspend: Suspend a bridging technology.  (Priv: <none>)
BridgeTechnologyUnsuspend: Unsuspend a bridging technology.  (Priv: <none>)
Challenge: Generate Challenge for MD5 Auth.  (Priv: <none>)
DAHDIDialOffhook: Dial over DAHDI channel while offhook.  (Priv: <none>)
DAHDIDNDoff: Toggle DAHDI channel Do Not Disturb status OFF.  (Priv: <none>)
DAHDIDNDon: Toggle DAHDI channel Do Not Disturb status ON.  (Priv: <none>)
DAHDIHangup: Hangup DAHDI Channel.  (Priv: <none>)
DAHDIRestart: Fully Restart DAHDI channels (terminates calls).  (Priv: <none>)
DAHDIShowChannels: Show status of DAHDI channels.  (Priv: <none>)
DAHDITransfer: Transfer DAHDI Channel.  (Priv: <none>)
Events: Control Event Flow.  (Priv: <none>)
ListCommands: List available manager commands.  (Priv: <none>)
Login: Login Manager.  (Priv: <none>)
Logoff: Logoff Manager.  (Priv: <none>)
PauseCall:  (Priv: <none>)
Ping: Keepalive command.  (Priv: <none>)
PRIDebugFileUnset: Disables file output for PRI debug messages  (Priv: <none>)
PRIDebugSet: Set PRI debug levels for a span  (Priv: <none>)
PRIShowSpans: Show status of PRI spans.  (Priv: <none>)
QueueChangePriorityCaller: Change priority of a caller on queue.  (Priv: <none>)
QueueClean: Clean up the seat status of the queue  (Priv: <none>)
QueueReload: Reload a queue, queues, or any sub-section of a queue or queues.  (
Priv: <none>)
QueueReset: Reset queue statistics.  (Priv: <none>)
QueueRule: Queue Rules.  (Priv: <none>)
Queues: Queues.  (Priv: <none>)
QueueStatus: Show queue status.  (Priv: <none>)
QueueSummary: Show queue summary.  (Priv: <none>)
WaitEvent: Wait for an event to occur.  (Priv: <none>)
```

Figure 11: AMI Command Example

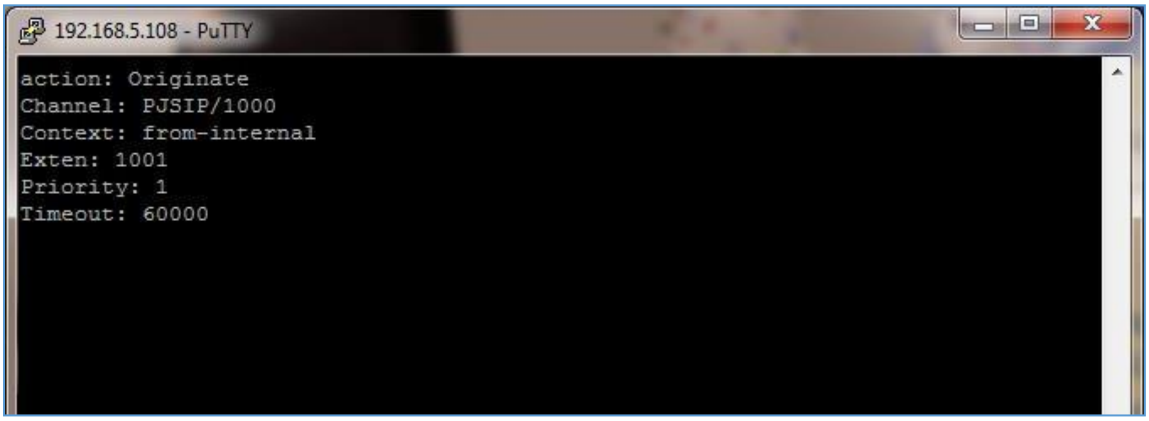
EXAMPLES

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. Onlyone 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.

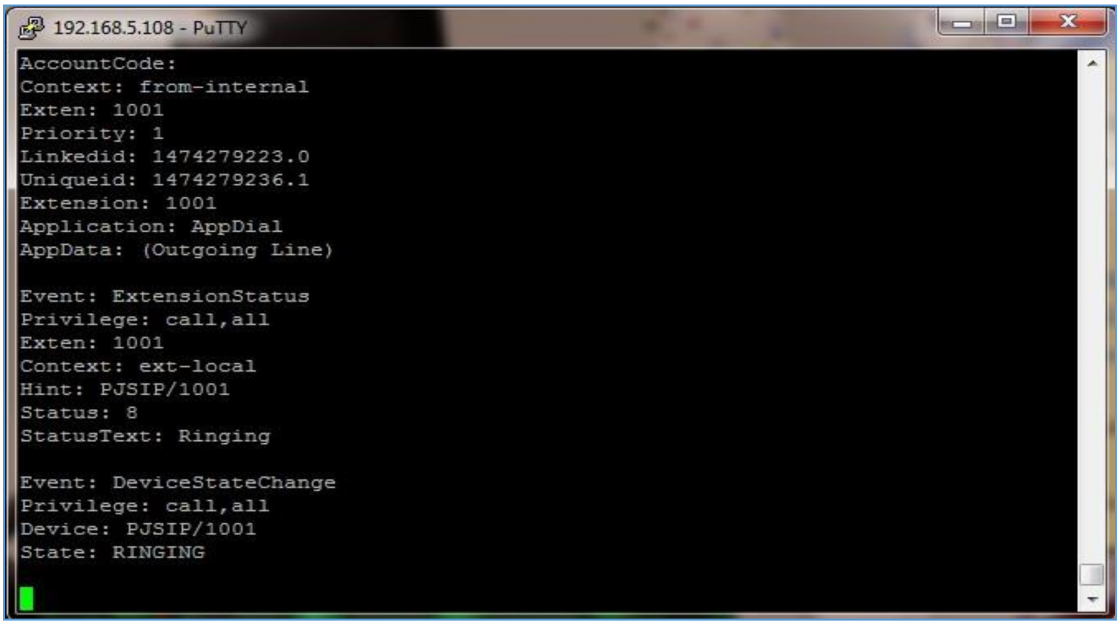
Note: Please make sure the AMI user is logged in and authenticated first

Example 1: Originate an internal call



```
action: Originate
Channel: PJSIP/1000
Context: from-internal
Exten: 1001
Priority: 1
Timeout: 60000
```

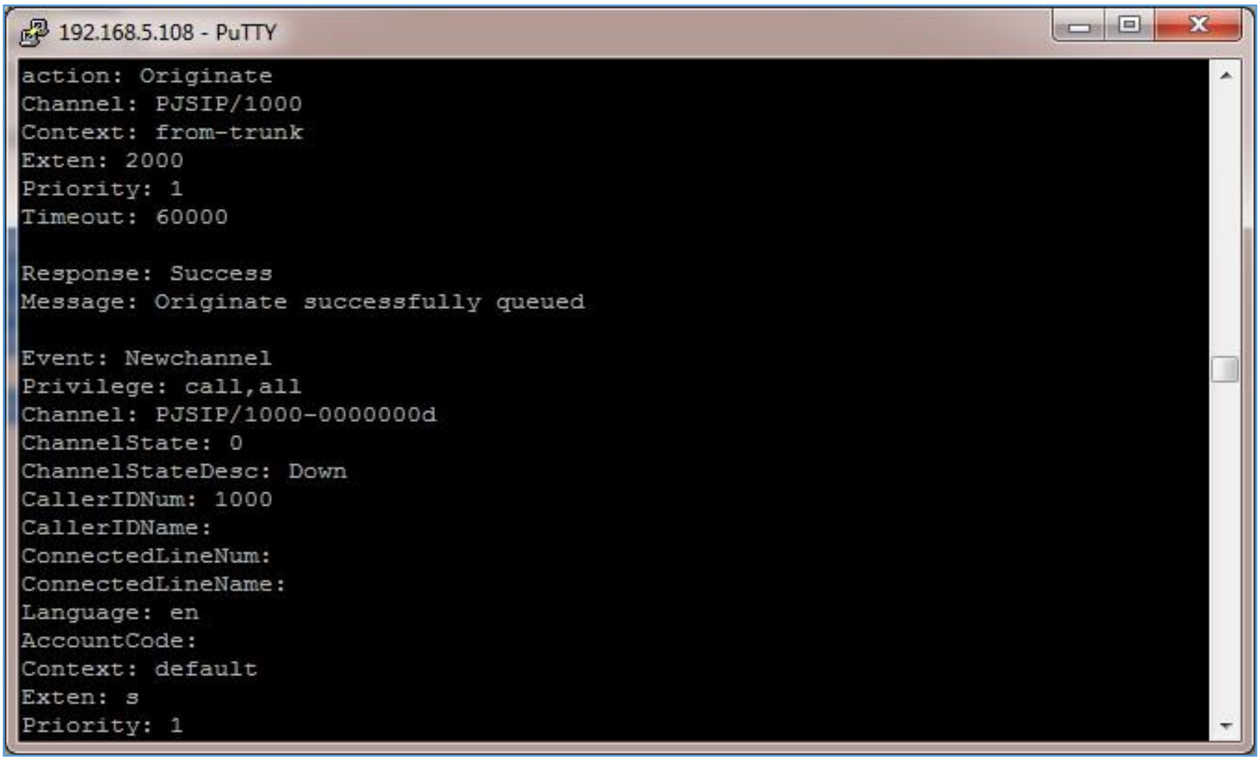
Figure 12: Example 1 - Originate Internal Call Ext 1000 to Ext 1001



```
AccountCode:
Context: from-internal
Exten: 1001
Priority: 1
Linkedid: 1474279223.0
Uniqueid: 1474279236.1
Extension: 1001
Application: AppDial
AppData: (Outgoing Line)

Event: ExtensionStatus
Privilege: call,all
Exten: 1001
Context: ext-local
Hint: PJSIP/1001
Status: 8
StatusText: Ringing

Event: DeviceStateChange
Privilege: call,all
Device: PJSIP/1001
State: RINGING
```

Figure 13: Example 1 - Ext 1001 Ringing

Example 2: Originate an external call via trunk

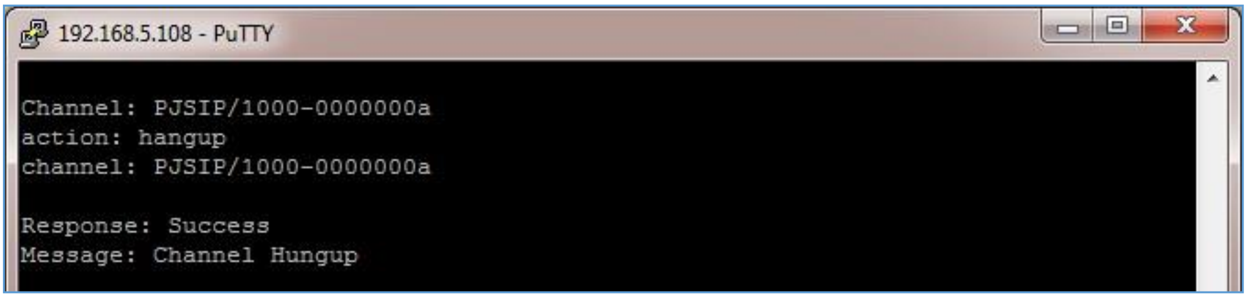


```
action: Originate
Channel: PJSIP/1000
Context: from-trunk
Exten: 2000
Priority: 1
Timeout: 60000

Response: Success
Message: Originate successfully queued

Event: Newchannel
Privilege: call,all
Channel: PJSIP/1000-0000000d
ChannelState: 0
ChannelStateDesc: Down
CallerIDNum: 1000
CallerIDName:
ConnectedLineNum:
ConnectedLineName:
Language: en
AccountCode:
Context: default
Exten: s
Priority: 1
```

Figure 14: Example 2 - Originate External Call

Example 3: Channel hang-up

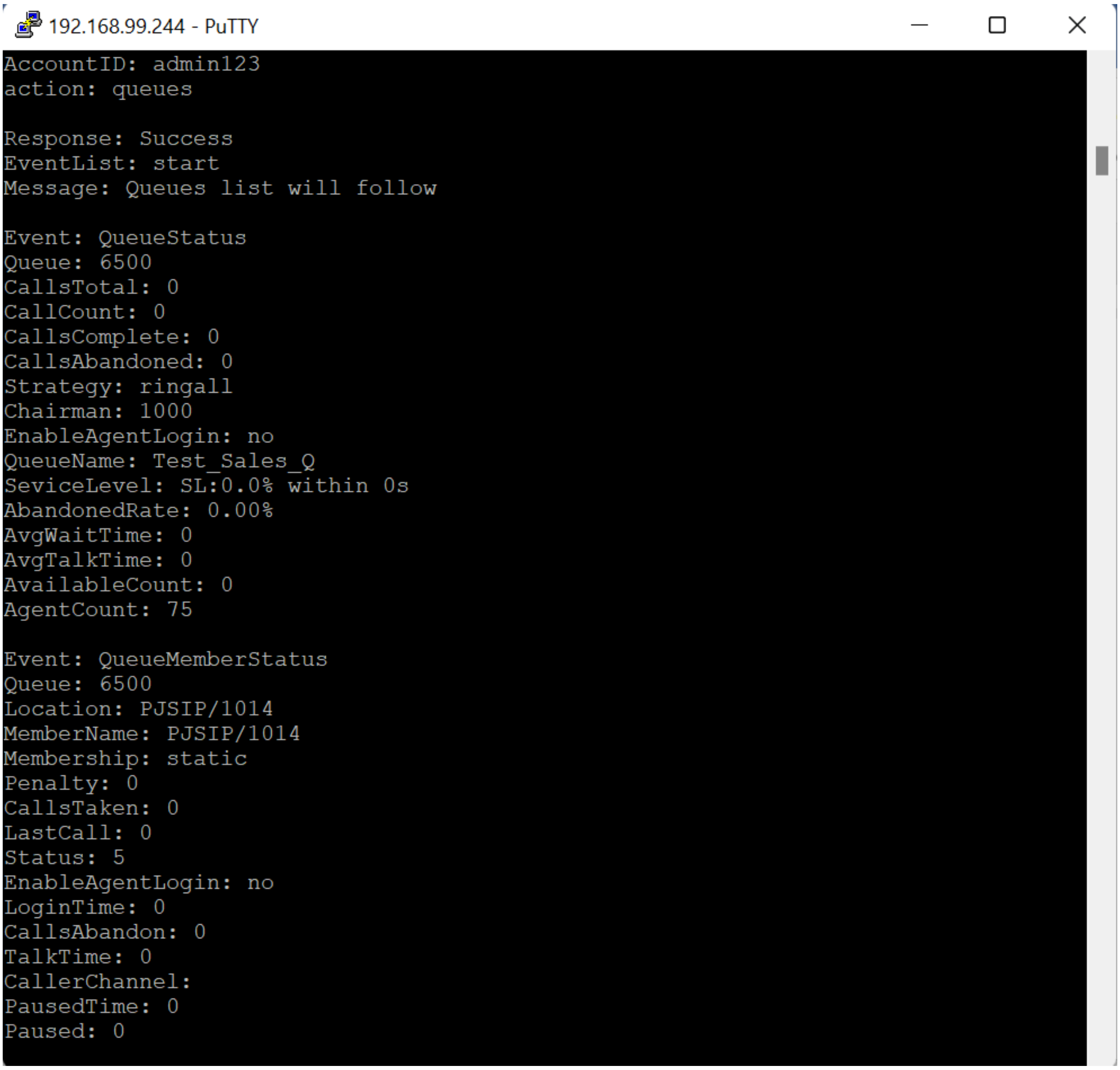
Note: This command will hang up active call.



```
Channel: PJSIP/1000-0000000a
action: hangup
channel: PJSIP/1000-0000000a

Response: Success
Message: Channel Hungup
```

Figure 15: Example 3 - Channel Hangup

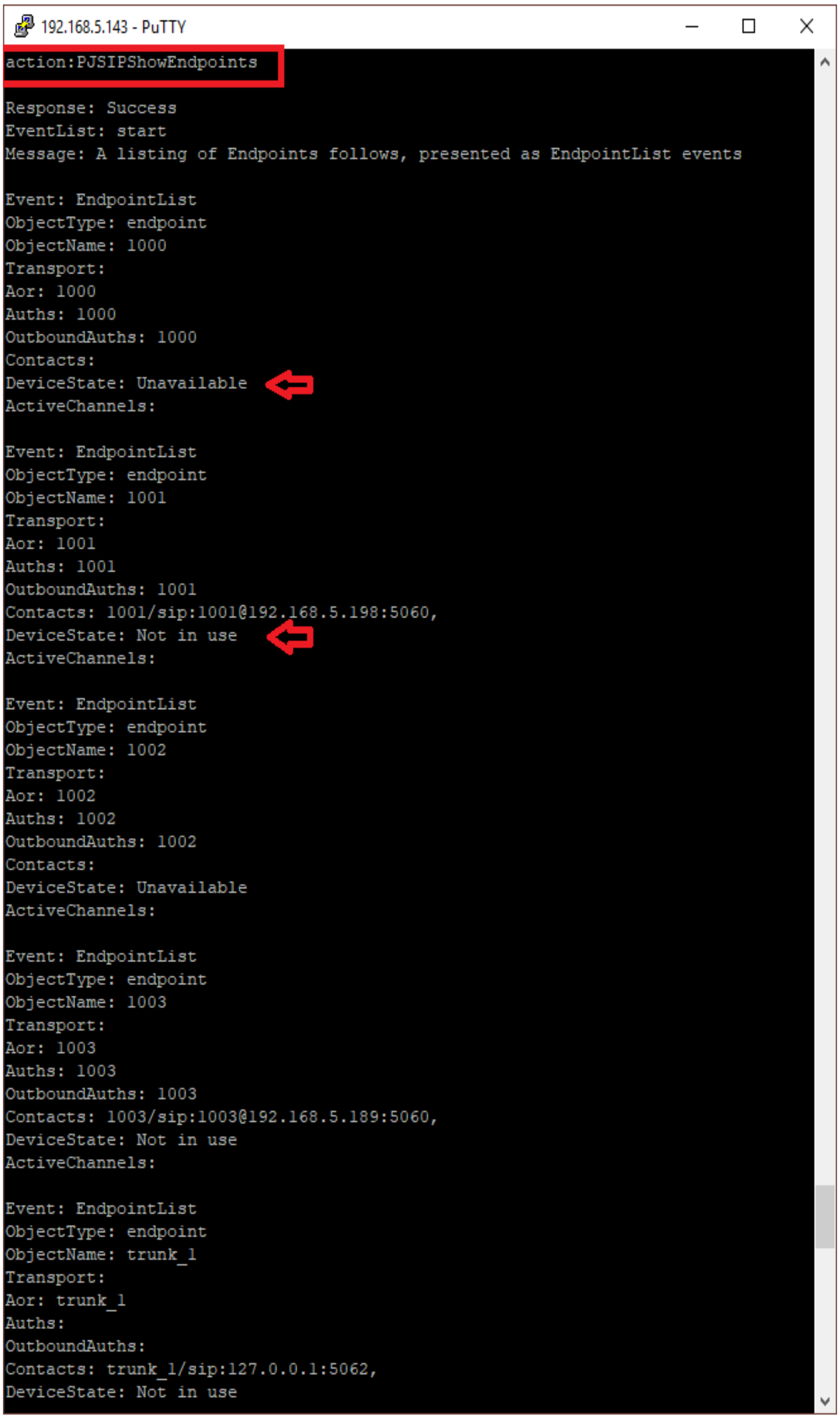
Example 4: Query the status of queue



```
AccountID: admin123
action: queues

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

Event: QueueStatus
Queue: 6500
CallsTotal: 0
CallCount: 0
CallsComplete: 0
CallsAbandoned: 0
Strategy: ringall
Chairman: 1000
EnableAgentLogin: no
QueueName: Test_Sales_Q
SeviceLevel: SL:0.0% within 0s
AbandonedRate: 0.00%
AvgWaitTime: 0
AvgTalkTime: 0
AvailableCount: 0
AgentCount: 75

Event: QueueMemberStatus
Queue: 6500
Location: PJSIP/1014
MemberName: PJSIP/1014
Membership: static
Penalty: 0
CallsTaken: 0
LastCall: 0
Status: 5
EnableAgentLogin: no
LoginTime: 0
CallsAbandon: 0
TalkTime: 0
CallerChannel:
PausedTime: 0
Paused: 0
```

Figure 16: Example 4 - Queue Status

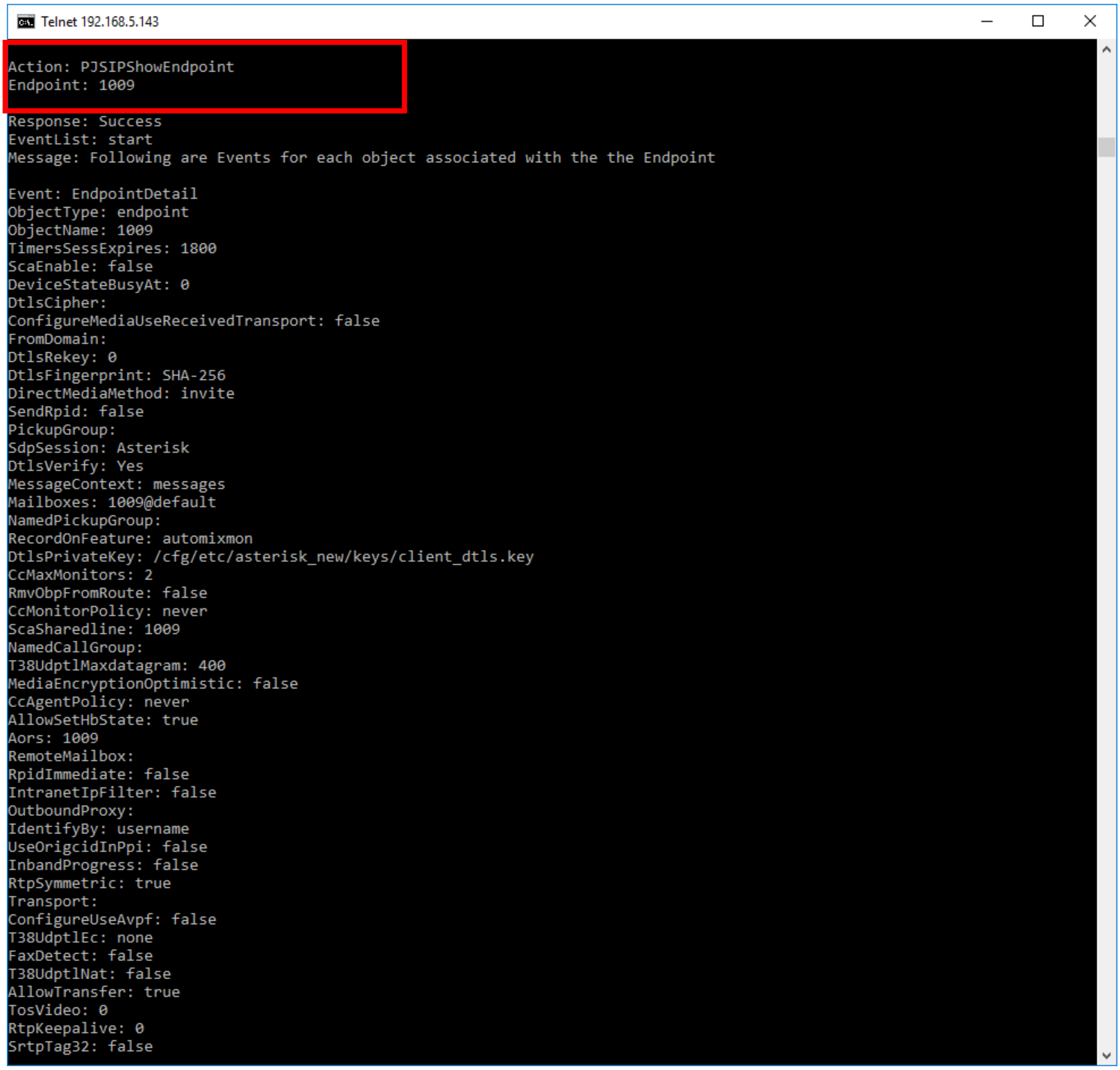
Example 5: PJSIPShowEndpoints query to get extensions and trunks status



```
action:PJSIPShowEndpoints

Response: Success
EventList: start
Message: A listing of Endpoints follows, presented as EndpointList events

Event: EndpointList
ObjectType: endpoint
ObjectName: 1000
Transport:
Aor: 1000
Auths: 1000
OutboundAuths: 1000
Contacts:
DeviceState: Unavailable
ActiveChannels:

Event: EndpointList
ObjectType: endpoint
ObjectName: 1001
Transport:
Aor: 1001
Auths: 1001
OutboundAuths: 1001
Contacts: 1001/sip:1001@192.168.5.198:5060,
DeviceState: Not in use
ActiveChannels:

Event: EndpointList
ObjectType: endpoint
ObjectName: 1002
Transport:
Aor: 1002
Auths: 1002
OutboundAuths: 1002
Contacts:
DeviceState: Unavailable
ActiveChannels:

Event: EndpointList
ObjectType: endpoint
ObjectName: 1003
Transport:
Aor: 1003
Auths: 1003
OutboundAuths: 1003
Contacts: 1003/sip:1003@192.168.5.189:5060,
DeviceState: Not in use
ActiveChannels:

Event: EndpointList
ObjectType: endpoint
ObjectName: trunk_1
Transport:
Aor: trunk_1
Auths:
OutboundAuths:
Contacts: trunk_1/sip:127.0.0.1:5062,
DeviceState: Not in use
```

Figure 17: PJSIPShowEndpoints Command

Example 6: PJSIPShowEndpoint query to get specific endpoint details



```
Action: PJSIPShowEndpoint
Endpoint: 1009

Response: Success
EventList: start
Message: Following are Events for each object associated with the the Endpoint

Event: EndpointDetail
ObjectType: endpoint
ObjectName: 1009
TimersSessExpires: 1800
ScaEnable: false
DeviceStateBusyAt: 0
DtlsCipher:
ConfigureMediaUseReceivedTransport: false
FromDomain:
DtlsRekey: 0
DtlsFingerprint: SHA-256
DirectMediaMethod: invite
SendRpid: false
PickupGroup:
SdpSession: Asterisk
DtlsVerify: Yes
MessageContext: messages
Mailboxes: 1009@default
NamedPickupGroup:
RecordOnFeature: automixmon
DtlsPrivateKey: /cfg/etc/asterisk_new/keys/client_dtls.key
CcMaxMonitors: 2
RmvObpFromRoute: false
CcMonitorPolicy: never
ScaSharedline: 1009
NamedCallGroup:
T38UdptlMaxdatagram: 400
MediaEncryptionOptimistic: false
CcAgentPolicy: never
AllowSetHbState: true
Aors: 1009
RemoteMailbox:
RpidImmediate: false
IntranetIpFilter: false
OutboundProxy:
IdentifyBy: username
UseOrigcidInPpi: false
InbandProgress: false
RtpSymmetric: true
Transport:
ConfigureUseAvpf: false
T38UdptlEc: none
FaxDetect: false
T38UdptlNat: false
AllowTransfer: true
TosVideo: 0
RtpKeepalive: 0
SrtpTag32: false
```

Figure 18: PJSIPShowEndpoint Command

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