Mizu VoIP Server HTTP interface

January 04, 2014

The Mizu VoIP server can be controlled by third party applications by the following ways:

1. *direct database manipulation with SQL commands (by ADO or ODBC) –described in "Database Interface"*
2. *via its TCP command interface "admin" port - documented in the "Admin Guide"*
3. *easy to use HTTP interface for simple class5 functionalities (described in this document)*

The server has a built-in basic web server waiting **for HTTP GET or POST request** (currently the GET method is recommended). By default the http listening port is 8084. This can be changed by the httpserver global config option.
A few useful functionalities can be accessed through this interface like callback, phone to phone calls, sms, etc.
Command format: xmapi/COMMAND?key=SERVERKEY&PARAMETERS
The parameters are not URL encoded. The basic ASCII character set are used.
Most of these functions are available also by SMS requests when the SMS text must contain the same parameters as described below.

The following values are defined for **COMMAND**:

- p2p -phone to phone call request
- sms -send sms message
- cb -initiate callback call
- balance -credit request
- rating –rate request
- addcredit –add credit (Only from trusted IP set by httpapiallowedip2)
- adduser–add new prepaid enduser (Only from trusted IP set by httpapiallowedip2. For more control use the DB API)
- charge –recharge using recharge PIN
- cli -add pin less number (ANI)
- db –any database query (select,update,etc) only if authenticated user type is admin
- oop –any operation defined on the console API (Command passed by the txt parameter)
- empty value -action will be guessed from parameters

The **key** is specific for each server instance. You can get/set it by server configuration "httpapikey".

The following **parameters** are defined:

- usr: username to authenticate the request
- usrid: id from tb_users (can be used instead of username)
- pwd: password to authenticate the request
- pin: used for pincode base authentication (after the rule set by the callingcardauth config option)
- md5auth: use md5auth instead of pwd on not trusted links. This must be calculated using MD5(rD58s + : + username + : + password+:+salt) (rd58s is a hardcoded value, salt is the value set by the httpapimd5salt global config option. The + operator means string concatenation)
- anum: A number (number 1) if applicable*
- bnum: B number (number 2) if applicable*
- txt: when sending text if applicable (for example for SMS)
- credit: used for the addcredit operation and adduser operations
- u_username: used for the adduser operations
- u_password: used for the adduser operations
- u_name: used for the adduser operations (optional)
- u_email: used for the adduser operations (optional)

*Sometime you have to use only one phone number. In that case the anum should be used. When the command requires two phone number, then both anum and bnum is used (for example P2P call requests)

The “now” word must be appended after the request string.
Response for this requests is OK or ERROR:reason in clear text (http body). The HTTP response code is 200 OK for valid requests or the corresponding error code (error codes are between 400 and 600) if the httpstrictresponse is set to true. Otherwise 200 OK will be returned for all valid requests.

Common HTTP return codes:
200: "OK" –command completed successfully
406: "Not Acceptable" –invalid command
403: “Forbidden” –wrong authentication
404: "Not Found" –user not found
420: "Bad Extension" –usually for PIN errors
421: "Extension Required" –number parameter is missing
412: "Conditional Request Failed" –command failed to be completed

The various functions can be called with the following parameters:

general
username password number1, number2
pincode number

general requests will result in a p2p call when at least 2 number are known. If only one number is know, than as a result it will generate a callback to that number. Two numbers can be supplied by sms number, and another number can be known from the sender CLI.

callback:
username password number (username and password based authentication and the number to be called)
pincode number (pincode based authentication and the number to be called)

register new number:
username password number
pincode number

phone to phone:
username password number1 number2
pincode number1 number2

add credit:
username password rechargecode number2
pincode rechargecode number2
rechargecode number2

balance request:
no parameter expected

add cli:
anum will be assigned for the user and can be used for A number based authentication

The following **global configuration options** are applicable (settable by using the Configurations form from the MizuManage):
httpserver: listening port for the built-in http server (default is 8084)
httpstrictresponse: whether to set the response also in the HTTP response code. If set to false (by default) then the HTTP response code will be 200 OK for all requests and the actual response have to be parsed from the response body.
httpsmscallbackip: allow SMS commands only for this ip (or multiple IP separated by comma). By default the value is empty which means all source address are allowed
httpapiallowedip: allow any command only from this IP. Empty by default which means all source are enabled.
httpapiallowedip2: allowed ip for sensitive operations (eg. addcredit). Requests from this ip (or multiple ip) can be sent without user password.
httpapikey: this key must be present in http requests otherwise they are rejected. By default this is empty which means that no key is required
httpapimd5salt: used for md5 checksum to make it more secure. Default value is 87159643
callingcardauth: define which fields are used for user authentication (by default the pin field is used). Pincode can represent the pin field of the user or the concatenated username and password (if allowed by callingcardauth). Use username/password instead of pincode whenever possible.
For callbacks you must define the campaign which will have the proper IVR content by the **defcallbackivr** global configuration setting. Read the IVR guide for more details.

Examples

Initiate callback:

http://domain.com:8084/xmapi/cb?key=KEY&usr=USRNAME&pwd=PWD&anum=PHONE1&now

Initiate phone to phone call:

http://domain.com:8084/xmapi/p2p?key=KEY&usr=USRNAME&pwd=PWD&anum=PHONE1&bnum=PHONE2&now

Sending SMS message:

http://domain.com:8084/xmapi/sms?key=KEY&usr=USRNAME&pwd=PWD&anum=PHONE1&bnum=PHONE2&txt=text&now

http://sip.mydomain.com:8084/xmapi/sms?key=1234&usr=1111&pwd=1111pwd&anum=2222&bnum=3630123456789&txt=Testsms&now

Request rate to destination:

http://domain.com:8084/xmapi/rating?key=KEY&usr=USERNAME&pwd=PWD&anum=PREFIX_OR_NUMBER&now

Request user credit:

http://192.168.1.7:8084/xmapi/balance?key=KEY&usr=USERNAME&pwd=PWD&now
or
http://192.168.1.7:8084/xmapi/balance?key=KEY&usr=USERNAME&md5auth=MD5CHECKSUM&now

Add credit: (from trusted IP only)

http://127.0.0.1:8084/xmapi/addcredit?key=KEY&usr=USERNAME&credit=AMMOUNT&now
or
http://127.0.0.1:8084/xmapi/addcredit?key=KEY&usr=USERNAME&md5auth=MD5CHECKSUM&credit=AMMOUNT&now

For some request you don't necessarily have to pass the password parameter if your configuration is set so. (Sending the password unencrypted on an untrusted network is a security risk!)

Web interface functions

You can automatically login also the web interface and access a few pages directly.
Don't confuse the built-in HTTP API with the web interface.
-The HTTP API was discussed above and served by a built-in http service in the mserver service (listening on port defined by the "httpserver" config option which is 8084 by default)
-The Web interface is implemented in a separate service (MizuWebService) which provides a user interface for the endusers, resellers, etc.

The following parameters can be used with the web interface:
function: name of the page (callhistory, tariffs, recharge) or "login"
username: sip username
password: password in clean text (use md5 and salt instead of clean password)
md5: md5 checksum calculated as MD5("C8y5:" + username + ":" + password+":"+salt) (don't include " and +)
salt: any salt value to be used for md5 calculation

Example:
http://domain.com?function=callhistory&username=Demo123&md5=1680f0c8aea2ee2e3cec77318c22311b&salt=92624f

For more details use the Admin Guide or contact our support.

Copyright © 2010-2014 MizuTech