User authorization

Users and devices will be allowed to access the system (and create new dialogs) only if they pass basic authorization which can be set from MManage -> Users and Devices -> Edit tab.
For IVR access the server will authenticate the actual enduser based on the A number or will request a PIN code.

Basic authorization

Dialog authentication can be performed in the following ways:
-Open Relay: if you set the NeedAuth to 0 for a user, then your server becomes an open relay (this is forbidden by the "enforcestrongauth" global config by default)
-Authentication based on IP address: for this you have to set NeedAuth to 1 and enter the peer IP address in the AuthIp field (can be a list of ip address separated by comma). Instead of IP address you can also use a domain names here.
-Authentication based on tech prefix: this is mainly used in h323 network. Set the NeedAuth to 2 and enter a valid techprefix for the user (which is usually a traffic sender)
-IP and techprefix: NeedAuth must be set to 3. The "TechPrefix" and "AuthIp" fields must be set correctly
-Username/password authentication: usually for your sip endusers. NeedAuth must be set to 4. Username and password fields must be accordingly
-Authentication based on username: A number authentication. NeedAuth must be set to 5 and with a valid username
-IP and port based authentication: gives you better security than just IP authentication and also it is useful when you have more traffic sender from the same domain. NeedAuth must be set to 6. Port and IP have to be set accordingly. (port is stored in the callsigaddr field in tb_users. You need to edit it if needed)
-Username and IP: both username and ip authmust match

**SIP endusers are usually authenticated based on username and password.*
**Traffic senders (carriers) are usually authenticated based on IP address.*

Access numbers

Access numbers are special users. You will have to create them like usual users but their ivrid have to be set to a valid campaign id. (which is then linked with an IVR script)

For callback access you also need to set the “iscallback” user field properly. Read the “callback” services for more details.

IVR authentication

For IVR calls the server will do a “callingcardauth” global config option based authentication.
Please note that in this case the caller device is already authenticated based on basic authorization settings. The IVR needs to find an enduser to allow further operation, like call forward.

The server can authenticate the user based on the following methods:

- ANI/CLI authentication: if the CLI is known and this method is allowed.

A number authentication can be used to try user authentication for a call coming from a traffic sender. If user is found with the actual A number then the caller will be authenticated as the enduser, otherwise will be authenticated as traffic sender. In this case you can require a PIN number from the user.

Configuration options:
anumberhandling global configuration

- 0=disabled
- 1=only add
- 2 = only accept
- 3=add and accept (default)
- 4=only a number access (no pincode request)

enableanumberlookup per user configuration. You need to set it to 1 for traffic senders (by default is set to 0 which means disabled)

A numbers can be also registered by the users on a web interface or by sending an SMS in the proper predefined format.

- PIN (calling-card) based authentification:

When the A number is not known or the A number based authentication is disabled, the IVR have to ask the user for a valid PIN code. This can be done by the CallingCardAuthentication IVR action.

After the server collects the DTMF digits it will lookup the database for a valid user entry. The authentication can be based on username, password or username+password or depending on the "**callingcardauth**" global config option which can have the following values:

- 0=calling card username or enduser username + password or enduser username + pin (default)
- 1=callingcard username
- 2= callingcard password
- 3= callingcard username+password
- 4=any username
- 5=any password
- 6=any username+password
- 7=any username+password or username+pin
- 8=username for callingcard and username+password or username+pin for other users (default)
- 9=pin
- 10=password or pin

User rights

User rights can be further restricted by several configuration option.
The most useful tool for this is the **routing** table. You can define were a certain user or a user group can initiate calls.

The following restrictions can be applied per user:
Allowedusers: list of the users or groups (prefixed with 'g') that is allowed to call the user. This can be used to restrict the access to an access number for example.

AllowedPartners: comma separated list of allowed partners and traffic senders. '*' will allow all. You may restrict the access on gateway or simpacket level instead of setting it for all simcards separately. Try to use the packet "allowedpartners" setting and leave it as '*' for the simcards!

Enabledprefixes: can be one prefix (with any length) or a list of prefixes with 3,4 or 5 digit separated by comma.
Can be used for trafic senders and gateways too. No need to setup a separate routing pattern if you use this restriction.
EnabledTechPrefixes: enabled techprefixes for the specified gateway (3 digit length numbers separated by comma)

BlockPrefixes: list of called prefixes that will be blocked for the user (techprefix will not be considered here). Numbers listed here must have 7 digit length and separated with comma.

MaxLines: max concurrent calls allowed (separate value for peak or offpeak)

Maxmonthlycredit: max allowed credit/month even if the user is postpaid

Maxmonthlycreditend: max Maxmonthlycredit (because we increase Maxmonthlycredit by maxmonthlycreditinc every month if the user was active)
Onlylocalaccess: traffic sender traffic will not be forwarded (can call only local users from tb_users and tb_numbers)
Maxmonthlycreditinc: determines how much money we add to Maxmonthlycredit every month

Access Rights: specify wich fielss are allowed for the user in the VPC application

0: simcard and traffic sender fields are not shown
1: simcard related fields are not shown (simid, packetname)
2: traffic sender related fields are not shown (name, username)
3: all fields are shown

Global configuration options:
MAXSPEACHLEN: max allowed call duration in sec
allowedusers: max ring time in sec
callmaxwait: max waittime allowed for operators between calls (for administrative purposes)
enforcestrongauth: enforce authorization and strong passwords

Try to avoid prioritizations by users, gateways, simpackets or channels (absolutepriority, priority, allowedpartners, prioritypartners, etc)
Almost all kind of configuration can be set up by using only the “routing” form.