Using the AETA SIP server

Contents

1. Introduction - Prerequisites and procedure

If you wish to use the SIP service of AETA, this document describes the procedure for registering codecs or other agents and setting up links between them.

The purpose of the service is to establish IP audio links between *SIP agents*. A SIP agent can be:

- A codec from AETA: Scoopy+, Scoop 5, ScoopFone, ScoopTeam ranges…
- A VoIP telephone, or a "softphone" (IP telephony application).
- A third-party codec that is compliant with N/ACIP and thus compatible with AETA codecs.
- Another SIP agent registered on the server and with which you wish to set up a link.

The first step is to configure every agent and register it on the server.

Afterwards, from each agent you can set a call to another agent registered as well on the server.

For each unit/agent, you must have a "SIP account" on AETA's server. Each account features an exclusive user **Number** which identifies it, and a **Password** that is used for authentication.

The AETA server handles various types of SIP accounts:

- Integrated "**Factory account**": such account is definitely bound to a unique product, and its data are permanently stored inside the product. *This kind of account is available on some types of AETA codecs (see chapter 2).*
- **"Premium" account**, subject to a subscription: the exclusive data for this account are provided at the time of subscription; you should keep them safe and keep the password secret. Compared to the integrated accounts, additional services are available, as described further in chapter 5.
- The other accounts are reserved for test numbers, temporary use, etc. Their operation is similar to premium accounts but they don't benefit from additional services.
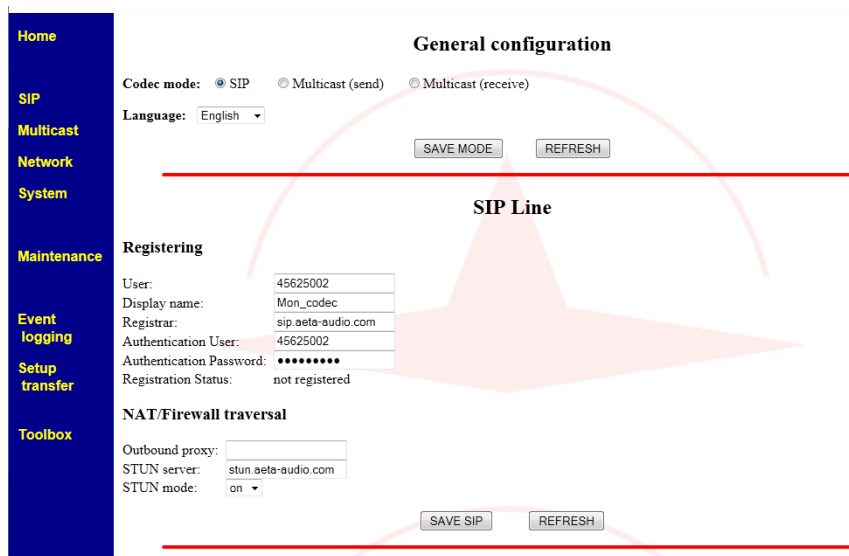
2. Configuring the SIP agent

This configuration consists in setting up the agent with parameters allowing it to register on the SIP server. The data are kept in the agent so it is not necessary to do this again afterwards.

Each time the agent boots or connects to the network, it contacts the server, identifies and authenticates itself, and is then *registered*: the server is aware of its presence and location.

Reminder: the very first step is to set up the agent for connecting to the network! Refer to its literature as needed.

2.1. Setting up a Scoop 4+

First connect the Scoop 4+ to the network and take note of its IP address. The configuration is done by using its embedded html pages: from a computer connected on the same local area network, open an html browser and enter the IP address of the Scoop 4+ in the "address" or "URL" field. This grants access to the html server embedded in the Scoop 4+. Click the SIP button and enter the data as in the example below:

User:	Enter here the user number provided with the SIP account.
Display name:	Some remote agents can display this field when a link is set ; you can enter any desired name.
Registrar:	This is the URL of the AETA server; you can also enter **sip.aeta.com**, or the numeric IP address : **85.214.119.212** (*necessary if the agent cannot access a DNS server).*
Authentication User:	Enter here the user number provided.
Authentication Password:	Enter the password provided with the SIP account.
STUN server:	You can also enter **stun.aeta.com**, or the numeric address : **85.214.119.212** (or use another STUN server)
STUN mode:	Select "on"

Click "Save SIP" to apply the data; if the Scoop 4+ is connected to the network and the link with the server works correctly, "Registration Status" should indicate "registered" after a while. If needed, use the "Refresh" button to check the status again; it can also be read from the menu using the unit's front panel interface.

2.2. Setting up a Scoopy+, Scoop 5 or Scoop 5 IP

We describe here the configuration using the embedded html pages, but it is also possible to use the keypad-display interface of a Scoopy+ or a Scoop 5.

First connect the codec to the network and take note of its IP address. From a computer connected on the same local area network, open an html browser and enter the IP address of the codec in the "address" or "URL" field. This grants access to the html server embedded in the codec Click "LOGIN", then "NETWORK" tab, "AOIP PARAMETERS", and enter the data as below (an example for a Scoopy+):

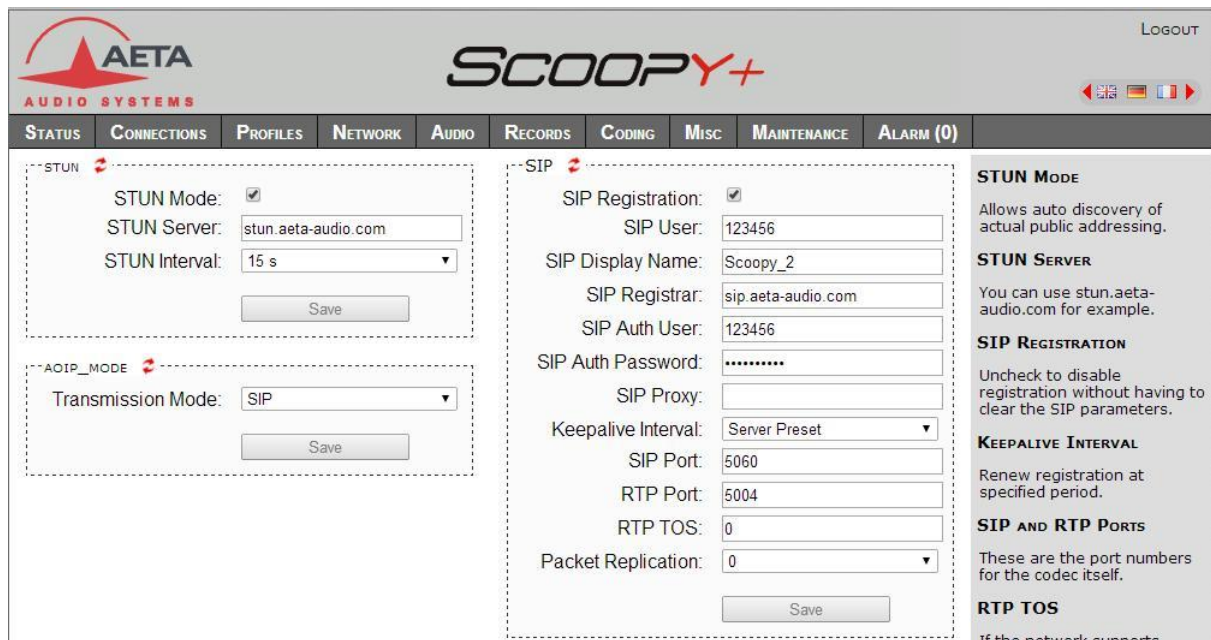|	
STUN Mode:	Check.
STUN Server:	**stun.aeta.com** can be used as well, or the numeric address: **85.214.119.212** (or use another STUN server).
STUN Interval:	Leave the default value unless you have reasons to do otherwise.
SIP Registration:	Check.
SIP User:	Enter here the user number provided with the SIP account.
SIP Display Name:	Some remote agents can display this field when a link is set ; you can enter any desired name.
SIP Registrar:	This is the URL of the AETA server ; you can also enter **sip.aeta.com**, or the numeric IP address : **85.214.119.212** (*necessary if the agent cannot access a DNS server).*
SIP Auth. User:	Enter the user number provided with the SIP account.
SIP Auth. Password:	Enter the password provided with the SIP account.
SIP Outbound Proxy:	(optional) if such server is available from your site, enter here its domain name or IP address.

Click "Save" to apply the data, and come back to the "STATUS" page; if the unit is connected to the network and the link with the server works well, "SIP status" should indicate "Registered" after a while. This is also visible via the front panel menu.

2.3. Setting up a Scoopy+ S, Scoop5 S, Scoop5 S-IP or µScoop

2.3.1. Using the "factory" account

A pre-integrated account is available on the recent versions of these products, manufactured after April 2017:

- Scoopy+ S, Scoop5 S or Scoop5 S-IP with firmware 1.07.03 or later.
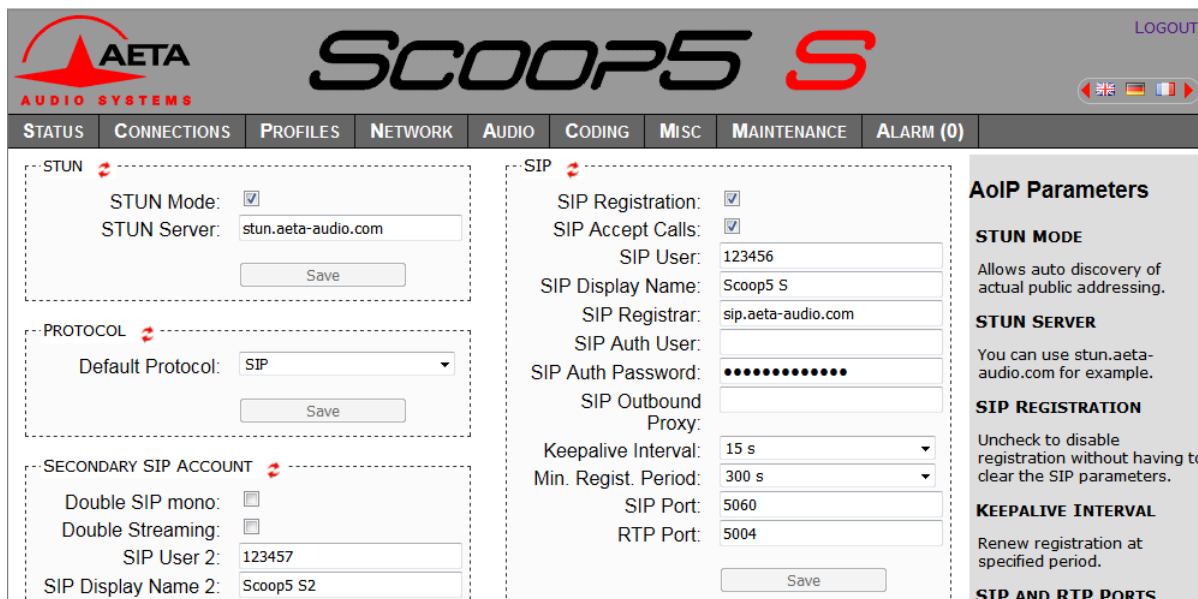- µScoop with firmware 1.03.01 or later.

For using this account you just need to reload this SIP account:

- Via the front panel interface (for Scoopy+ S or Scoop5 S):
  Tools / **Misc** / **Reset** / **Factory SIP Account**
- Using the embedded html pages:
  tab **MAINTENANCE**, page **RESET**, check "Factory SIP Account" and click "**Reset**".

2.3.2. Using a "premium" account

We describe here the configuration using the embedded html pages, but it is also possible to use the keypad-display interface of a Scoopy+ S or a Scoop5 S.

If you have got a premium SIP account that you want to configure the unit with, here is the procedure: first connect the codec to the network and take note of its IP address. From a computer connected on the same local area network, open an html browser and enter the IP address of the codec in the "address" or "URL" field. This grants access to the html server embedded in the codec. Click "LOGIN", then "NETWORK" tab, "AOIP PARAMETERS", and enter the data as below in the "**SIP**" frame (an example for a Scoop5 S):

STUN Mode:	Check.
STUN Server:	**stun.aeta.com** can be used as well, or the numeric address: **85.214.119.212** (or use another STUN server).
SIP Registration :	Check.
SIP User :	Enter here the user number provided with the SIP account.
SIP Display Name :	Some remote agents can display this field when a link is set ; you can enter any desired name.
SIP Registrar :	This is the URL of the AETA server ; you can also enter **sip.aeta.com**, or the numeric IP address : **85.214.119.212** (*necessary if the agent cannot access a DNS server).*
SIP Auth. User:	Leave empty or enter the user number again.
SIP Auth. Password :	Enter the password provided with the SIP account.
SIP Outbound Proxy:	(optional) if such server is available from your site, enter here its domain name or IP address.

If you have got a second account to register (for operating the unit as a double SIP codec or for Double Streaming), enter its data in the "SECONDARY SIP ACCOUNT" frame on the left part of the page.

Click "**Save**" to apply the data, and come back to the "STATUS" page; if the unit is connected to the network and the link with the server works well, "SIP status" should indicate "Registered" after a while. This is also visible via the front panel menu.

2.4. Setting up a ScoopFone 4G

2.4.1. Using the "factory" account

The ScoopFone 4G features a permanent SIP account on the AETA server. To activate it, reload this SIP account via the front panel interface: **TOOLS** / **Reset** / **SIP account.**

2.4.2. Using a "premium" account

If you have got a premium SIP account that you want to configure the unit with, the procedure is similar as for a Scoopy+ S or the Scoop5 S: refer to chapter 2.3.2 above, Using a "premium" account.

2.5. Setting up a ScoopTeam

2.5.1. Using the "factory" accounts

The ScoopTeam includes two pre-integrated SIP accounts on the AETA server. To activate them, reload these SIP accounts:

- Either via the front panel interface:
  Tools > Troubleshooting > Reset > Reload the Factory SIP accounts
- Or using the embedded html pages: **MAINTENANCE** tab, **RESET** page, check "Factory SIP Accounts" and click "**Reset**".

2.5.2. Using "premium" accounts

If you have got one or two premium SIP account(s) that you want to configure the unit with, the procedure is similar as for a Scoop5 S: refer to chapter 2.3.2 above, Using a "premium" account.

2.6. Setting up a MultiScoop (Codec module)

2.6.1. Using the "factory" accounts

Each Codec module of a MultiScoop includes two pre-integrated SIP accounts on the AETA server. To activate them, reload these SIP accounts using the embedded html pages:
MAINTENANCE tab, **RESET** page, check "Factory SIP Accounts" and click "**Reset**".

2.6.2. Using "premium" accounts

If you have got one or two premium SIP account(s) that you want to configure the unit with, the procedure is similar as for a Scoop5 S: refer to chapter 2.3.2 above, Using a "premium" account.

2.7. Other type of agent

SIP agents are numerous, and the designation of the fields to enter is not always exactly the same. It is not possible to describe here all the possible variations, but you can follow some basic rules:

- Use the *User Number* provided for fields such as *account, user, authentication name, authentication ID/user*, etc.
- Sometimes a full URI is required: this is in such case *number@sip.aeta-audio.com*, for instance *45625021@sip.aeta-audio.com*.
- Use sip.aeta-audio.com for fields such as *registrar*, *SIP proxy.*
- In doubt, look for the relevant information in the product literature or from the supplier.

3. Setting up a link

3.1. Network access conditions

Most often, the SIP agent does not access the Internet directly but rather via an access router or gateway, and possibly a firewall. Moreover, usually this comes with a network address translation (between the codec's local address and the public address on the Internet), called NAT.

The SIP server and the usage of STUN usually cope with this situation. However you should make sure that adverse conditions do not prevent the agent to access the network suitably; especially check that:

- The Internet access is not blocked by a firewall.
- UDP packets are not blocked, especially towards the server's SIP port 5060.
- The Internet access router does not perform undesired port redirections that might interfere with the operation. *Usually it is not necessary to set static port redirections on the access/firewall router.*

Whenever the Internet access goes through a restrictive firewall, a minimum of allowance is required for operating the SIP agent. See more details further in 6, Network security aspects.

3.2. Calls between agents

After switching the agent on and connecting it to the network, and if the connection with the SIP server works correctly, the agent should indicate "registered".

From this time it is ready to receive a call from a remote agent.

If we assume a remote agent is registered on the server under the number *45625043*: to call it, you should dial:

- The *SIP URI* of this agent, in our example *45625043@sip.aeta-audio.com*,
- Or simply its **number**: *45625043*. This is the only method for some agents.

3.3. Optionally disabling STUN

The above recommended settings normally allow the agents to exchange the audio streams directly with each other, without transiting through the SIP server. This ensures a more direct path through the network, and consequently a lower latency and a lower risk of packet loss.

However, there are situations in which this direct exchange will not work. This issue can be solved by relaying the audio streams via the server (for more details refer to 4.4, *RTP proxy feature*). This sometimes requires to *not* use STUN.

As a **simple rule**: make your first tests with STUN active. If one stream or the other does not seem to reach its destination, while the session negotiation completes correctly (the caller gets an answer from the called agent, but one unit or the other waits for synchronization indefinitely and/or hangs up after a while), then you should try to disable STUN.

⇨ To do that, on Scoop 4+ set "STUN mode" off (also possible via the front panel menu).
⇨ On the other AETA codecs, uncheck "STUN Mode" (or use the menu on the front panel).

Wait for the codec to re-register after this change, and then retry the call.

4. Complementary information and tools

4.1. Host server

The service is hosted in a data center on a dedicated server (TÜV certified, ISO 27001 standard). The service provides the quality and reliability guarantees expectable for a professional service:

- High availability with 24/7 monitoring.
- Redundant and backed up power.
- Dedicated and reliable equipment.

4.2. Numbers for tests

For first startup tests, you can call a test codec registered on the AETA SIP server :

15000 :   Codec permanently on and transmitting an audio program

This codec is available permanently as much as possible, but it can be stopped sometimes for maintenance reasons. It may also be busy at times.

To avoid this, please do not use this test codec for long duration tests! We reserve the right to release sessions set up with this codec, without preliminary notice and at any time.
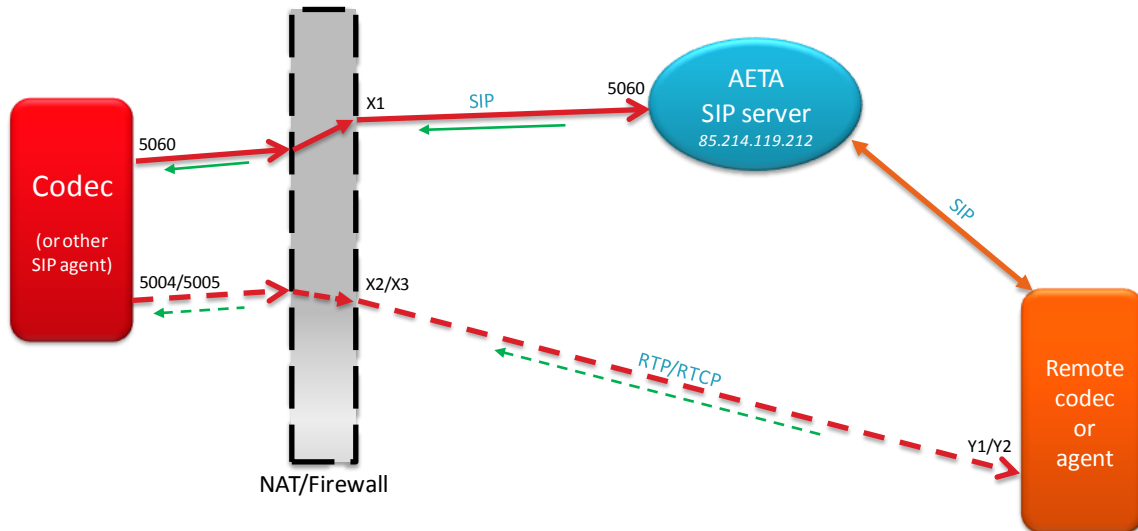
4.3. Alternate SIP port

Sometimes firewalls or routers specifically interfere with the Internet access for the SIP agents. In many cases such routers react to the agents using the 5060 UDP port. If you believe you are, or might be, in such situation, you can try an alternate, non standard, SIP port (5070) on the AETA SIP server.

To use this option with an AETA codec, you just have to specify this port by entering, in the "SIP-Registrar" field, the value "sip.aeta-audio.com:5070", or "85.214.119.212:5070".

Do not confuse the SIP port of the server, set as mentioned above, and the SIP port of the codec. On an AETA codec, the latter port is defined by the "SIP port" parameter; it is rarely useful to change it.
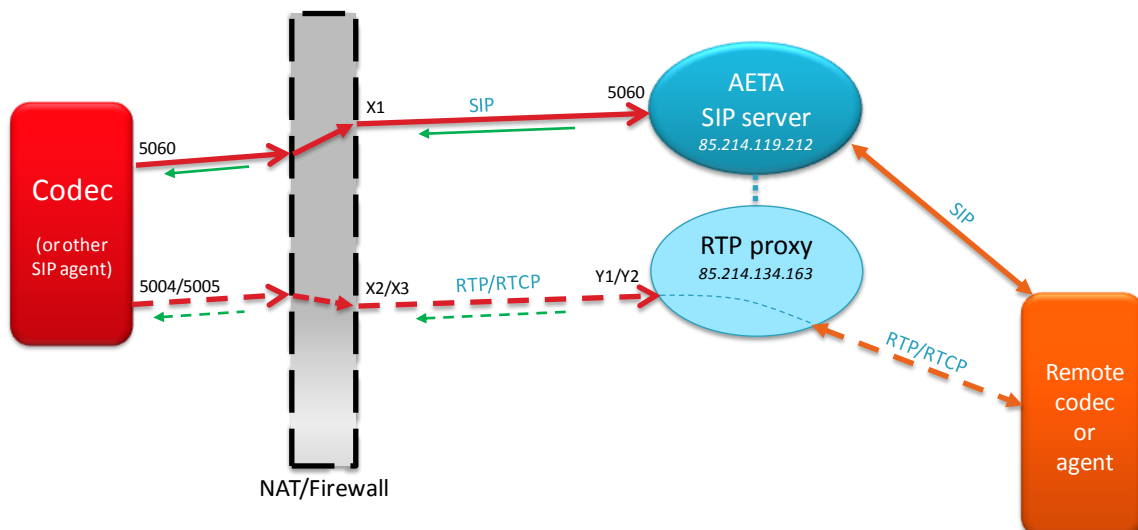
4.4. RTP proxy feature

On a SIP session, the agents *a priori* try to exchange audio streams directly with each other, each agent notifying the other the IP address and port to which the audio stream (RTP protocol) should be sent. This process can be hampered when the Internet access router implements network address translation (NAT). Thanks to the use of STUN, the SIP agent can detect its public IP address and port numbers, and manage to get this direct peer to peer exchange, as shown in the diagram below.

Using STUN, direct RTP exchange between agents

However, there are situations in which this direct exchange will not work, for instance when the NAT router is of so-called "symmetric" type. Such case is often met with mobile network access.

To workaround this issue, the server includes an "RTP proxy" function that can handle the routing for the RTP streams. When the server detects a network configuration that requires this, it involves in the transaction an RTP proxy which will relay the RTP streams, as shown in the diagram below.

RTP exchange relayed by the RTP proxy

It is often necessary to disable STUN (at least on one of the agents) so that the server can accurately detect the context which requires involving the RTP proxy.

The RTP proxy efficiently solves critical NAT issues, and with a rather simple operation. However, obviously this "detour" via the proxy has some drawbacks because it tends to increase the distance and/or the number of routers crossed on the path between the agents:

- Increased transport delay, and consequently latency.
- Possible increase in the jitter and the packet loss rate.

For these reasons, and for getting the most direct route possible, we recommend this two-step approach as described before (3.3, Optionally disabling STUN):

1. Use STUN and try to establish the link.
2. If the network connectivity does not allow such direct connection to work correctly, disable STUN, and then the RTP helps get a successful link.

If you prefer to get a fast and almost guaranteed result, you can disable STUN right away.

4.5. Backup server

To maintain service in all circumstances, the server is secured by a backup server, which is permanently active. In case of a failure of the main server, or for a maintenance action, the service can make a "hot" switchover to the backup server, while keeping all functions identical.

- No specific configuration has to be performed on the agents to benefit this redundancy.
- No user action is needed in the event of a switchover; the switch to backup is automatic and transparent.
- At the time of switching, there may be a disturbance for links which were running prior to the switchover. In the worst case, the link can be dropped if it was relayed through the RTP proxy (which is backed up as well). A new call will re-establish the link immediately.

4.6. Alternate RTP proxy

A second RTP proxy, located in France, is also available as an alternative to the nominal RTP proxy. It allows to benefit from an optimized route when the agents involved in a link via the RTP proxy are both located in France. More generally, this proxy provides a shorter path for agents located in the most western part of Europe.

To force the use of this proxy (instead of the nominal proxy), the procedure is quite simple: in the SIP registration settings ("AoIP parameters") of the agent that will launch the calls, enter **sip.aeta-audio.fr** as "registrar". Afterwards the operation is just the same as usual.

- *Beware for the "factory" account: reloading it also reloads the standard setting for the registrar (sip.aeta-audio.com), and thus brings back the standard RTP proxy.*
- *However, if you use the "factory" account, you can edit the "registrar" field and replace it by sip.aeta-audio.fr.*
- *Reminder: there is no obligation for the two agents of a link to be registered with the same registrar domain name; the same AETA service is accessed whatever the domain name (sip.aeta-audio.com, sip.aeta.com, sip.aeta-audio.fr), or if using the numeric address 85.214.119.212.*
- *The domain name set on the agent that receives the call has no influence on the selection of the RTP proxy.*

5. Additional features of the premium service

Premium accounts are subject to a yearly subscription. They bring along a number of additional services.

5.1. Number structure

The SIP numbers allocated to premium accounts follow some simple rules:

- The numbers allocated to these accounts include 8 digits.
- When a customer subscribes several accounts, these feature a common 4-digit prefix, specific to the subscriber (e.g. 4567). After this prefix, numbers are assigned sequentially starting from 5001 (e.g. 45675001, 45675002, etc.).
- In case additional accounts are subscribed later, these new accounts continue the sequence after the numbers already assigned to the same subscriber.

The prefix is the basis for many of the functions below. In the following, we call "group" the numbers/accounts sharing a common prefix.

5.2. Portability

A premium account can be used on any SIP agent, provided that this agent is compatible with the server. The data may be transferred into another agent if necessary.

Be careful, nevertheless, not to use by mistake the same account on two agents at the same time! This would cause a wrong and unpredictable operation. Make sure to clear up the data on the previous agent after such a transfer.

5.3. Short numbering

For calling a number inside the same group, you can dial just the last 4 digits.

Examples:

- 45675412 calls 45675002 : call sent to 45675002
- 45675412 calls 5002 : call sent to 45675002
- 45995005 calls 5002 : call sent to 45995002

5.4. "Incoming calls" blocking

Optional service, on request. Applies to the whole group.

When this feature is activated, the server does not relay to the group calls which are originated from agents not belonging to the group.

Example, if we assume that incoming calls blocking is activated for the group 4567xxxx:

- 45675412 calls 45675002: the call is submitted to 45675002
- 45995005 calls 45675002: the call is blocked by the server.

Warning: calls originating from factory accounts are also rejected in all cases.

5.5. "Outgoing calls" blocking

Optional service, on request. Applies to the whole group.

When this feature is activated, the server does not forward calls sent by a member of the group towards agents that do not belong to the group, except 15000 (which stays open for testing).

Example, if we assume that outgoing calls blocking is activated for the group 4567xxxx:

- 45675412 calls 45675002 : the call is routed
- 45675412 calls 45995033 : the call is blocked by the server
- 45675412 calls 902080 : the call is blocked by the server
- 45675412 calls 15000 : the call is routed (exception)

Warning: calls sent to factory accounts are also rejected in all cases.

5.6. Self-management of passwords

Optional service, on request. Applies to the whole group.

When this service is selected, AETA provides for every SIP account an on-line access to the server (login+password) that allows to edit *ad libitum* the password of the SIP account.

Don't mix up the password for this login and the SIP account password!

Summary instructions for use:

- Log into the account management interface :
  https://sip.aeta-audio.fr/siremis/user/login
- *Username* = SIP account number, *Password* = that provided by AETA
- Menu *Own SIP Profile / Subscriber data* : *Edit* for editing password and/or e-mail
- Menu *Own SIP Profile / Location Records:* information on the current registration
- Menu *Accounting / Call Data Records:* list of calls originated by the number

5.7. Quarterly call log

Optional service, on request. Applies to the whole group.

When this service is selected, AETA provides the subscriber, on each calendar quarter, a log of the calls:

- Set from a number in the group and/or to a number in the group.
- That were successful (unsuccessful calls are not logged)
- Initiated or terminated within the quarter.

The data are provided in a file in csv format, including especially for each call the begin date/time, duration, calling number and called number.

The file is delivered by e-mail to the technical contact of the subscriber.

5.8. Hunting group

Optional service, on request. Applies to the whole group.

When this service is selected, AETA provides the subscriber a "hunting group number" and an additional series of accounts (in same count as the regular numbers) that can be used as a hunting group.

- A call sent to the hunting group number is forwarded by the server to the first number of the additional series;
- If [the unit at] this number is absent or busy, the call is forwarded to the second number in the additional series;
- And so on, up to the last number of the additional series.
- The additional series is specifically devised for this feature and it cannot, for instance, set outgoing calls.

For example, for the group with prefix 4567, the hunting group number is 45676000.
From a codec of the same group, it is also possible to simply dial 6000.

The numbers for the additional "hunting group" series are assigned sequentially starting from 6001 (e.g. 45676001, 45676002, etc.).

5.9. Information on the service

Each subscriber must provide to AETA an e-mail address of a technical contact.

Whenever needed, an e-mail is circulated to the technical contacts for announcing events or changes regarding the service:

- Evolution of the service, new features;

- Quarterly delivery of the call logs (when this option is subscribed);

- Possible operation events;

- Planned intervention on the servers, possibly implying a disturbance risk; such risk is always limited thanks to the available backup.

In the latter case, it is possible for a subscriber to perform a switchover at a self-decided moment (within a given time window). Doing so is more complex, but this can possibly avoid disturbance in a critical time period. AETA makes the users know about such alternative when it is available.

6. Network security aspects

It may be necessary to configure the access/firewall router of the LAN on which the agent is connected. This will depend on the nature and organization of this LAN.

6.1. Connection via a standard "box"

In this simple case, there is usually nothing to change, as there is no firewall rule that could block the SIP sessions. However:

- It may be useful to change the SIP port used on the server: see above in 4.3, *Alternate SIP port*. *You may also use directly the alternate port 5070.*

- Do not configure any static port redirection/forwarding; this is useless if not hazardous for the network security.

- It may be useful to change the codec's RTP port: for AETA codecs, this setting is also available in the "AoIP Parameters".

6.2. Operation in a company network

If the agent that is used is free to send UDP packets towards the Internet and receive returned UDP packets with no blocking, then you are on a similar configuration as the above case (standard box), and the same recommendations apply.

Conversely, if a firewall *a priori* blocks the Internet access from the SIP agent, access allowance rules must be set. At minimum the following must be done:

- Allow the agent to access the SIP port (UDP 5060 or 5070) of the sip.aeta-audio.com server (85.214.119.212), and accept returning SIP/UDP packets.

- For the audio streams (RTP/RTCP), allow the agent to send packets from its RTP port to the outside, and accept returning UDP packets.

Besides:

- It is not necessary to set the agent in a DMZ.

- It is not necessary to open incoming ports from the Internet, but it is just required to accept the return path on ports opened via NAT by outgoing packets.

- Do not configure any static port redirection/forwarding; this is useless if not hazardous for the network security. For example, a redirection of the public port 5060 to a codec can quickly give rise to attacks.

- No TCP port is required, except if you wish to remote control the codec (but this is not relevant for the audio exchanges).

6.3. How to enhance security

The above recommendations bring a reasonable security in most cases. You can further improve the protection by allowing *all exchanges* only with the SIP server, which will prevent any attack from a third party on an agent located in the local area network (On the other hand, this implies to always route streams via the RTP proxy, and consequently to somewhat lengthen the path of the RTP streams).

The following must be set on the firewall:

- Allow the agent to access the SIP port (UDP 5060 or 5070) of the sip.aeta-audio.com server (85.214.119.212), and accept returning SIP/UDP packets. Block SIP requests (UDP port 5060) towards any other server, and SIP requests from any other source than the server's address.

- For the audio streams (RTP/RTCP), allow the agent to send packets to the port range 55004 to 55999 on AETA proxy server (addresses 85.214.134.163 and 81.169.136.159[1]), and accept returning UDP packets. Block RTP streams to/from any other address.

Besides:

- Of course, don't set any agent in DMZ.
- No TCP port is required, except if you wish to remote control the codec (but this is not relevant for the audio exchanges).
- Disable STUN on the agents.

Other solutions exist to enhance even more the network security:

- Installation on the local network of an *Outbound proxy,* that will relay all SIP transactions and RTP streams, and will be the only device allowed to communicate with the server.

- Use of an SBC (Session Border Controller) dedicated to managing AoIP transactions with the outside, and integrating firewall functions for a maximum protection.

---

[1] The address of the alternate SIP proxy located in France is 51.75.25.240.

7. Troubleshooting

⇨ As mentioned above, in doubt regarding the configuration of an agent you should first refer to its documentation and/or supplier. AETA can provide specific support only for codecs and agents supplied by AETA.

⇨ Similarly, although we tested many products so far, we cannot guarantee the compatibility of a third party device or software.

⇨ If meting problems for registering an AETA codec or setting up a link, if possible download the event logs from the agent(s) and send them as attachment to an e-mail to sipserver@aeta-audio.com with a precise description of the test circumstances.

⇨ Whenever possible, provide as well a "Wireshark" log recorded at the interface of the concerned agent during a session or connection attempt.

8. Glossary

Term or abbreviation	Meaning
SIP Agent	Terminal entity capable to implement the SIP protocol and set up multimedia sessions with another agent.
AoIP	*Audio over IP*, audio via an IP protocol network
DNS	*Domain Name Server*. Performs the resolution of symbolic addresses into numeric addresses.
NAT	*Network Address Translation*. A NAT router typically allows to share one or a few public IP addresses for a local area network.
RTP proxy	Server capable to relay the RTP streams exchanged by the two SIP agents during a connection. This technique allows to workaround blockings due to very restrictive access routers.
SIP	*Session Initiation Protocol,* protocol used for signalling multimedia sessions.
Softphone	*Software Phone,* software on a PC or smartphone allowing to make telephone sessions via an IP network.
STUN	*Simple Traversal of UDP through NATs,* protocol allowing a client behind a NAT router to discover its public IP address and ports.
URI	*Uniform Resource Identifier,* identifier for a SIP "agent".