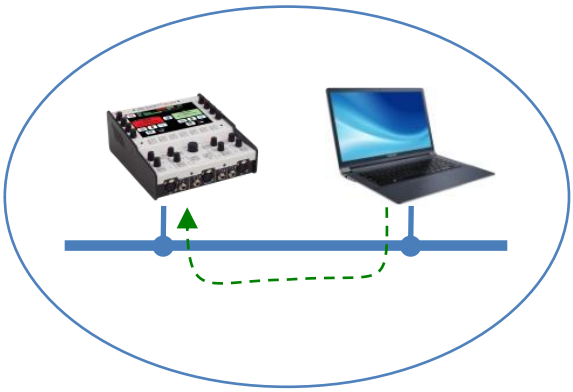
Using the AETA Remote Access service

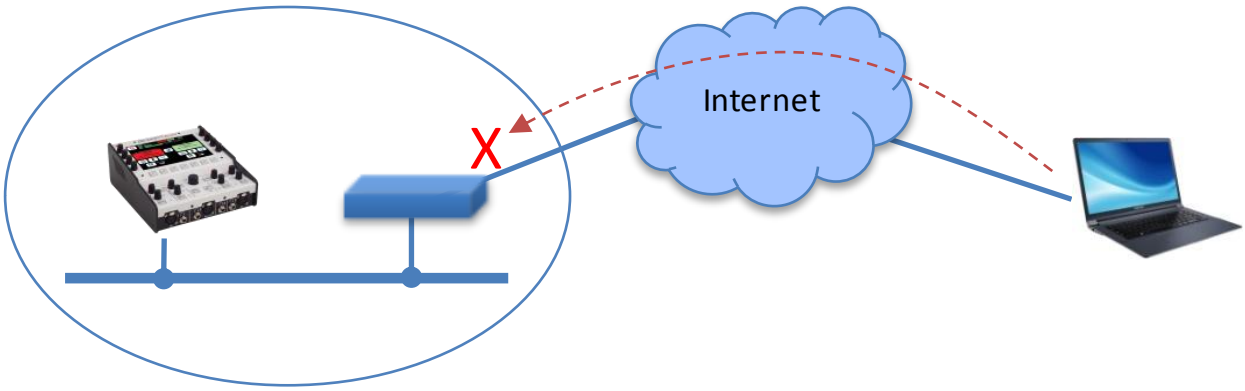
1. Background

AETA codecs can all be controlled via an IP interface, and for instance a computer can easily take control over a codec when it is connected on the same LAN as the unit:



The computer can access the embedded html pages of the codec. In the case of a ScoopTeam, the "My ScoopTeam LE" application is an even smarter alternative.

When the computer is on a remote location, connected via the Internet, there is most often a need to go through NAT router(s) and/or firewall(s):



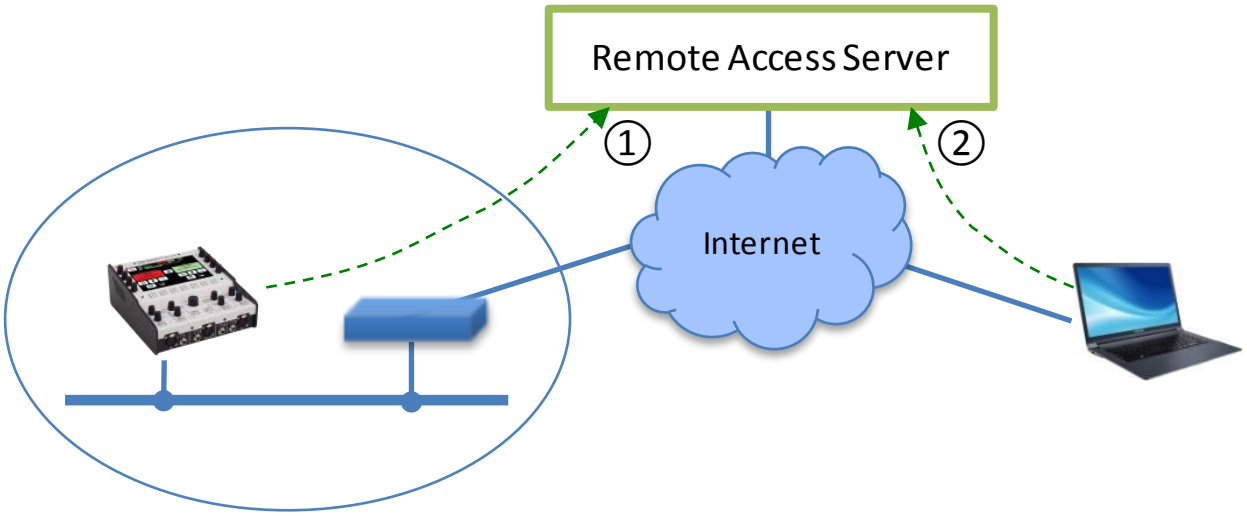
In such situation, it is not possible to get a connection as directly as over a LAN.

The AETA Remote Access service is designed for working around this obstacle and enabling to take control over a device even in such case[1].

[1] However, a very restrictive firewall can of course block the service

2. "Remote Access" service

The system relies on using a remote access server, as a intermediary between the codec and the control device. A control session is performed in two phases:



1. The codec connects to the server, and gets available for a possible remote access session.
2. A user who wants to remote control the codec sets a connection to the server, and the server sets a virtual link between the control device and the codec, identical in its operation to a direct link via a LAN.

The two connections are secured and encrypted.

Three types of links are proposed:

- Remote assistance: this service allows the AETA support staff to access the codec, for help or possible investigation. *Such operation cannot be performed without an activation on your part.*
- Remote html access: allows to access the html pages of the codec from remote. The control device can be any device with a web browser, without the need to install any application. *A "Remote Access" option must be installed on the codec for using this service.*
- "Remote access +": such link, available for a ScoopTeam with the "Remote access +" option, allows controlling the ScoopTeam from a Windows PC equipped with the "My ScoopTeam RE" application.

When the codec features more than one IP interface, it is possible to use for remote access an interface distinct from the one used for AoIP transmission.

Except for the "Remote access +" link type, all codecs from the following ranges are accessible via this service:

- ScoopTeam
- Scoopy+ S
- Scoop5 S et Scoop5 S-IP
- µScoop
- ScoopFone 4G, ScoopFone 4G-R, ScoopFone IP

The following chapters describe the operation for the various service types.

3. Using the remote assistance

3.1. Prerequisites

You just need to have the up-to-date firmware on the codec. No additional option is required.

The codec should have an Internet access, for instance via its Ethernet connection to a LAN. But other IP connections are suitable as well: mobile data access, Wi-Fi…

3.2. Connecting the codec to the server

You first need to connect the codec to the server to make it accessible. To do so, the procedure slightly varies depending on the product.

3.2.1. ScoopTeam

Menu **Tools** > **Remote Assistance**: activate "**Remote Assistance**".

*If a "Remote Access" option is installed, the menu is **Tools > Remote Access,** "**Remote Access**".*

In the same menu, you can select the IP interface to be used for the remote access connection: "**Interface for Control".** For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: menu **Status,** "**Remote Assistance Service".**

Take note of the MAC address of the main Ethernet interface (LAN1): menu **Network > LAN1 settings** .

3.2.2. Scoopy+ S or Scoop5 S ranges

Menu: **Tools > Maintenance > Remote Assistance**, **Allow Remote Access.**

*If a "Remote Access" option is installed, the menu is **Tools > Maintenance > Remote Access**, **Allow Remote Access.***

In the same menu, you can select the IP interface to be used for the remote access connection: "**Network Interface**". For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: menu **Tools > About** (item "Remote Access Status").

Take note of the MAC address of the Ethernet interface: menu **Tools > About**.

3.2.3. ScoopFone range (4G, IP, 4G-R)

Menu: **Tools > Rem. assist.**, **Enabled: Yes.**

*If a "Remote Access" option is installed, the menu is **Tools > Rem. access**.*

Selecting the IP interface to use for connecting to the service is only possible using the html pages: see further.

Check the successful connection: menu **Tools > Rem. assist.**

Take note of the MAC address of the Ethernet interface: menu **Ethernet**.

3.2.4. Via the html pages (all ranges)

Tab **MAINTENANCE**, page **REMOTE ACCESS**, check "Allow Remote Assistance".

*If a "Remote Access" option is installed, tab **MAINTENANCE**, page **REMOTE ACCESS**, check "Allow Remote Access".*

In the same menu, you can select the IP interface to be used for the remote access connection: "Network Interface". For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: **STATUS** tab, **GENERAL** section.

Take note of the MAC address of the Ethernet interface: **NETWORK** tab, **ETHERNET PARAMETERS** or **ETHERNET SETTINGS** page.

3.3. Assistance session

Tell the AETA technician the MAC address of the codec; this is the identifier for the device.

AETA can then set a control session over the codec. The link is secure and encrypted.

You may disable remote assistance once the intervention is over. *This is recommended for avoiding useless data traffic.*

4. Using the remote html access

4.1. Prerequisites

On the codec you should have available:

- The up-to-date firmware.
- The "Remote Access" option (or "Remote access +" option).
- Internet access, for example via its Ethernet connection to a LAN. However other IP connections are suitable as well: mobile data access, Wi-Fi…

The control device can be any device with a web browser (no need to install an application): computer, tablet, even a smartphone…

4.2. Connecting the codec to the server

You first need to connect the codec to the server to make it accessible. In order to restrict the access to the codec, you can define a "codec password" that will authorize its remote access.

***Note**: for security reasons, a password that is empty or too short is not accepted by the system (more about this in chapter 6.1 further).*

The procedure and settings slightly vary depending on the product.

4.2.1. ScoopTeam

Menu **Tools > Remote Access**: activate "**Remote Access**".

In the same menu, you can select the IP interface to be used for the remote access connection: "**Interface for Control".** For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: menu **Status,** "**Remote Access Service".**

If you want to change the password, you must be logged as an administrator (*if necessary, switch this via the menu **Tools > Access Level**: **Administrator***). In the menu **Tools > Remote Access** you can enter a password as you want, with following rules:

- The password must be at least 8 characters long (see above note and chapter 6.1 further).
- If you leave the password blank or enter one with less than 8 characters, a random password is automatically generated by the ScoopTeam.

4.2.2. Scoopy+ S or Scoop5 S ranges

Menu: **Tools > Maintenance > Remote Access**, **Allow Remote Access.**

In the same menu, you can select the IP interface to be used for the remote access connection: "**Network Interface**". For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: menu **Tools > About** (item "Remote Access Status").

If you want to change the password, go to the menu **Tools > Maintenance > Remote Access**, **Codec Password.** The following rules apply:

- The password must be at least 8 characters long (see above note and chapter 6.1 further).
- If you leave the password blank or enter one with less than 8 characters, a random password is automatically generated by the codec.

4.2.3. ScoopFone range (4G, IP, 4G-R)

Menu: **Tools > Rem. access**, **Enabled: Yes.**

Selecting the IP interface to use for connecting to the service is only possible using the html pages: see further.

Check the successful connection: menu **Tools > Rem. access**

If you want to change the password, you must use the embedded html pages: see below.

4.2.4. Via the html pages (all ranges)

Tab **MAINTENANCE**, page **REMOTE ACCESS**, check "Allow Remote Access".

In the same menu, you can select the IP interface to be used for the remote access connection: "Network Interface". For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: **STATUS** tab, **GENERAL** section.

You can enter a password as you want, with following rules:

- The password must be at least 8 characters long (see above note and chapter 6.1 further).
- If you leave the password blank or enter one with less than 8 characters, a random password is automatically generated by the codec.

4.3. Accessing the html pages

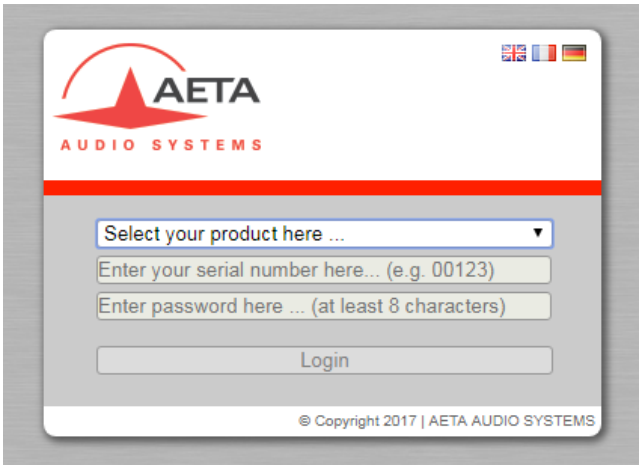
The unit to be controlled must be connected to the server, and you must know the following information about the device:

- Product type (example: Scoopy+ S)
- Serial number
- "Codec password"

Open a web browser, and go to the following URL:

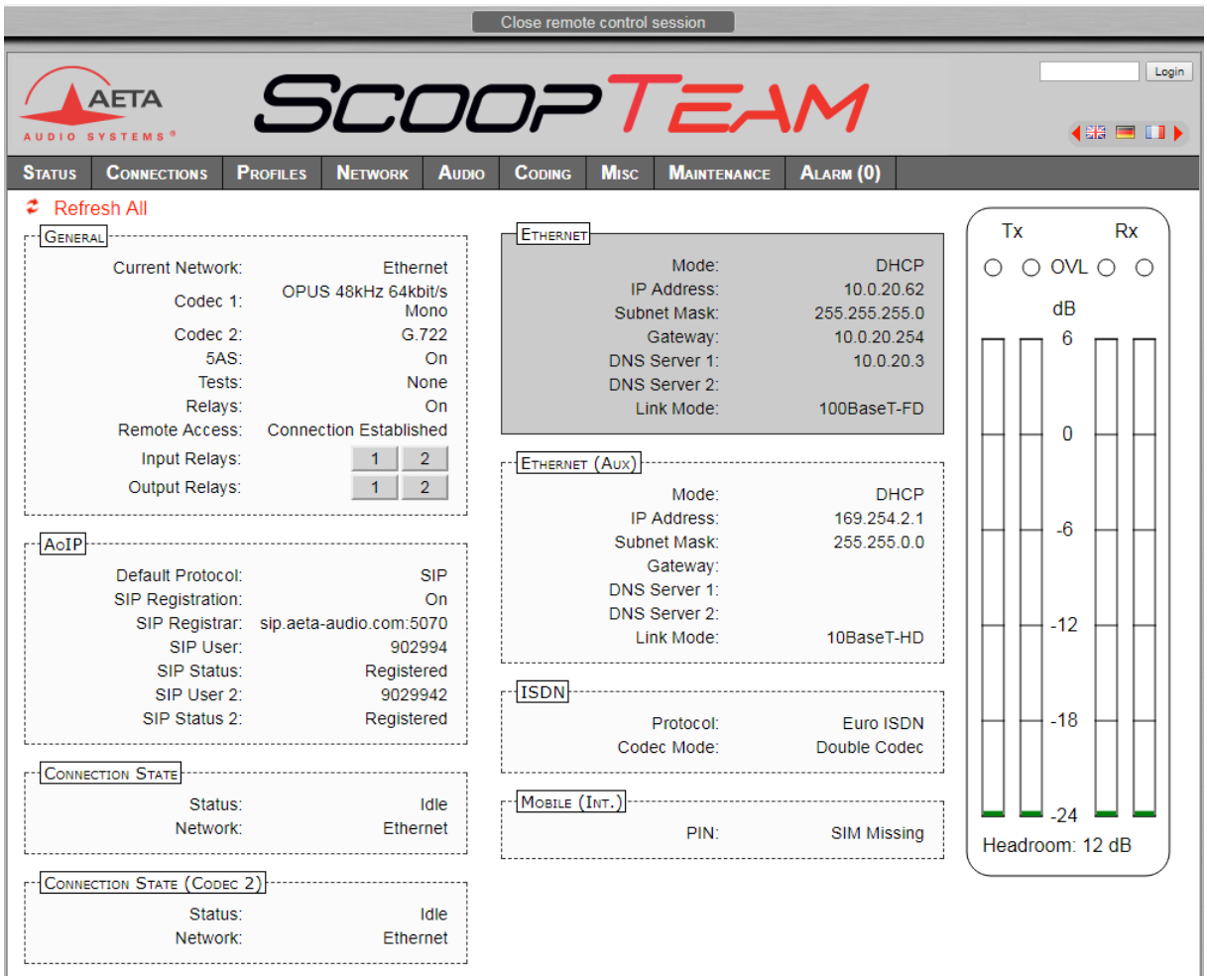
https://cloud.aeta.com/rac

You reach the AETA remote html access portal:



1. Select the product type from the drop-down list.
2. Enter the serial number (with or without the leading "0").
3. Enter the codec password.
4. Click the "Login" button.

After a while you get the home page of the codec, almost identical to that you would get with a direct connection over a LAN:



The difference is in the small bar at the top ("Close remote control session"). Click it when you wish to disconnect from the server.

Navigating the pages follow the same rules as a direct access through a LAN.

Warning: do not confuse the "password codec" that you used for this connection, and the password possibly configured to restrict the access to the html pages in a general way (i.e. regardless if the access is local or remote). These passwords are independent of each other.

The link is secured and encrypted.

You may disconnect the codec once the session is over. *This is recommended for avoiding useless data traffic.*

5. Using a "Remote access +" link

This feature is only available for a ScoopTeam. *A ScoopTeam with this capability can also be controlled by remote access to its html pages, as described in the previous chapter: please refer to this chapter for using this type of link.*

5.1. Prerequisites

On the ScoopTeam you should have available:

- The up-to-date firmware (1.03 or later).
- The "Remote Access +" option.
- Internet access, for example via its Ethernet connection to a LAN. However other IP connections are suitable as well: mobile data access, Wi-Fi…

The control device is a Windows PC, with the "My ScoopTeam RE" application installed.

You can download from AETA's web site the installation file for the application. Launch the installation file, and then open the instruction document that is installed along with the application. You can find there the instructions for using "My ScoopTeam RE".

5.2. Connecting the ScoopTeam to the server

As for the remote access service, you first need to connect the ScoopTeam to the server to make it accessible. In order to restrict the access to the codec, you can define a "codec password" that will authorize its remote access.

***Note**: for security reasons, a password that is empty or too short is not accepted by the system (more about this in chapter 6.1 further).*

Menu **Tools > Remote Access**: activate "**Remote Access**".

In the same menu, you can select the IP interface to be used for the remote access connection: "**Interface for Control".** For using always the same interface as the one for audio over IP transmission, select "Auto".

Check the successful connection: menu **Status,** "**Remote Access Service".**

If you want to change the password, you must be logged as an administrator (*if necessary, switch this via the menu **Tools > Access Level**: **Administrator***). In the menu **Tools > Remote Access** you can enter a password as you want, with following rules:

- The password must be at least 8 characters long (see above note and chapter 6.1 further).
- If you leave the password blank or enter one with less than 8 characters, a random password is automatically generated by the ScoopTeam.

5.3. Remote controlling with "My ScoopTeam RE"

Set up the virtual connection between the PC and the ScoopTeam, using its serial number as identifier, and its codec password for authentication. You can build a list of known devices and easily switch from one to another.

You can find the details for the operation in the instruction document that is installed along with "My ScoopTeam RE".

6. Security aspects

By its very principle, the remote access feature, as it makes possible remote control via Internet from any location, might imply security risks, for example:

- Undesired takeover of a device by an unauthorized person;
- Eavesdropping the transactions;
- Intrusion into a codec or a control device.

6.1. Protection measures

The AETA remote access system has several provisions to avoid these risks, including:

- The **connection between the codec and the server** is authenticated and encrypted (SSH).
- This connection requires a **voluntary activation** on the codec. As long as the feature is not activated, no one can take control of the codec via the Internet. The same is true for remote assistance and remote access by AETA staff. *For even more security, you may enable remote access only for the duration of an intervention.*
- The **connection between the control device and the server** is authenticated and encrypted (HTTPS and/or SSH).
- The **codec password** ensures that only authorized people can act on the codec, even when remote access is active. For this reason, an empty or short password is not accepted by the system. On the contrary, it is highly recommended to use a complex password. We recommend at least 13 characters, with a combination of uppercase and lowercase letters, numbers, and special characters among the following: _ - + * . : , ; # ? ! =.

6.2. Tips for firewalls

It is not necessary to create static routes or redirections from public ports to codecs (this is even not recommended), as it is the codec or the controller that initiates a connection to the server.

If a firewall prevents this connection, it may be necessary to enable packet exchanges with the AETA server: domain cloud.aeta.com (or, at the time of writing, the IP address 80.154.26.106).