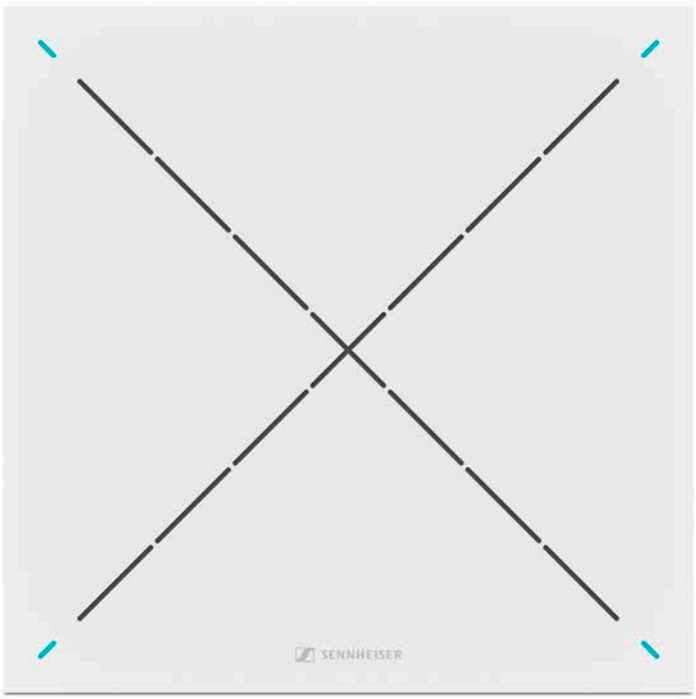


TeamConnect Ceiling 2

Configuration of 802.1X

Sennheiser electronic GmbH & Co. KG

Am Labor 1, 30900 Wedemark, Germany, www.sennheiser.com
AN 1258 v1.0

SENNHEISER

Contents

Prerequisites

For the 802.1X configuration of the TeamConnect Ceiling 2 ceiling microphone array (TCC2) some tools are needed:

- **SSH client tool**

  We recommend using the PuTTY SSH client or a standard command line SSH client. Any SSH client capable of openssh keys can be used.
- **SCP client tool**

  We recommend using the PuTTY SCP tool or a standard command line SCP client. Even though they are very popular, tools like WinSCP are not supported since they rely on more permissions than are granted (e. g. reading out the file system of the remote machine).
- **SSH keys (pnac_key pair + pnac-ft_key pair)**

  These keys are provided by Sennheiser on the following website:

  www.sennheiser.com/tcc2

For the 802.1X configuration two things need to be done in parallel:

1. Configuration (see „Configuring 802.1X“)
2. Transfer of the needed files by SCP (see „Transferring files to the TCC2“)

Connecting to the TeamConnect Ceiling 2

To configure 802.1X for the TCC2, a secure shell (SSH) session needs to be established. For this task an SSH client tool is needed. If a graphical tool (GUI) is preferred, PuTTY (https://www.putty.org/) can be recommended since it is available for multiple platforms and was tested to work with the TCC2. Linux systems come with a preinstalled SSH client for the command line (Console). Both ways are described in this manual.

For an SSH connection to the TCC2, an SSH key pair is mandatory. You can download it from the following website:

www.sennheiser.com/tcc2

These keys should **not** be considered a security measure. They are publicly available and are **not confidential**. They are only needed to explicitly start the 802.1X configuration of the TCC2.

During the 802.1X configuration the user will later set his own password for reentering the 802.1X configuration.

Network connection

The first step is setting up the network connection. The TCC2's default configuration is auto-IP mode. This means a DHCP client is waiting for an IP address to be assigned. If you operate a DHCP server in the network, on which the 802.1X configuration should be performed, refer to the configuration or logs of the DHCP server to obtain the TCC2's IP address. If no DHCP server is present on the network, the TCC2 will use a link-local address in the area of 169.254.0.0/16.

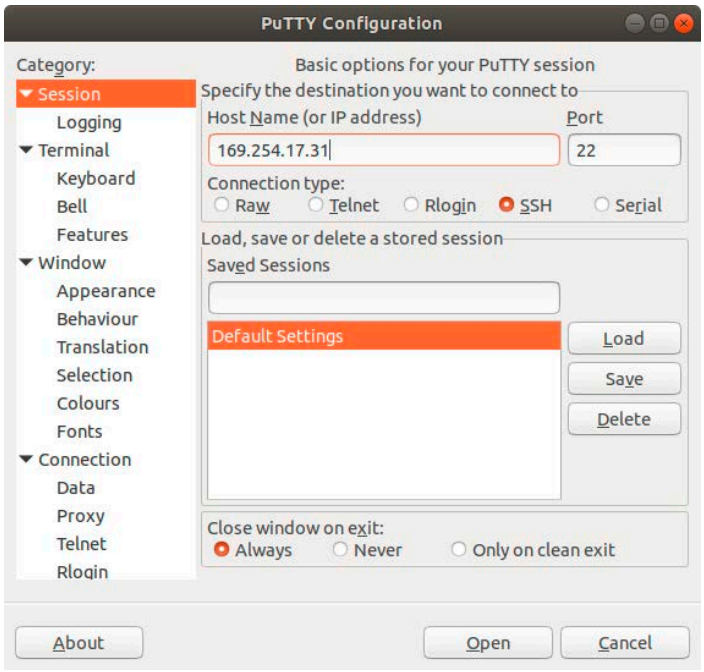
In both cases (DHCP or link-local) the TCC2 will publish its hostname and IP address via multicast DNS (mDNS).

For a more convenient discovery and network setup of the TCC2 you can use the Sennheiser Control Cockpit software (www.sennheiser.com/control-cockpit-software).

Once the IP address of the TCC2 is known, you can verify the IP connection by sending pings to the TCC2. If the TCC2 replies, you can continue with the next steps.

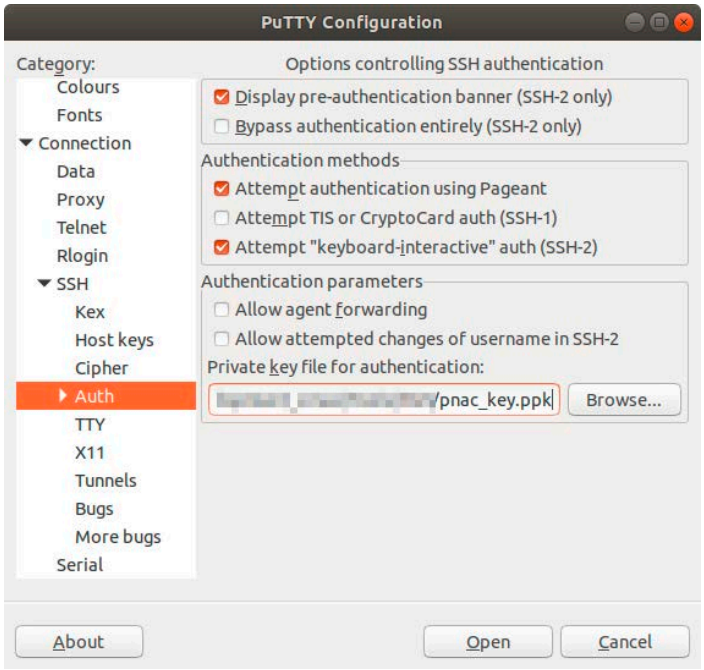
SSH Connection with PuTTy

In PuTTY there are three options which need to be set. On the left you can navigate through the configuration categories.

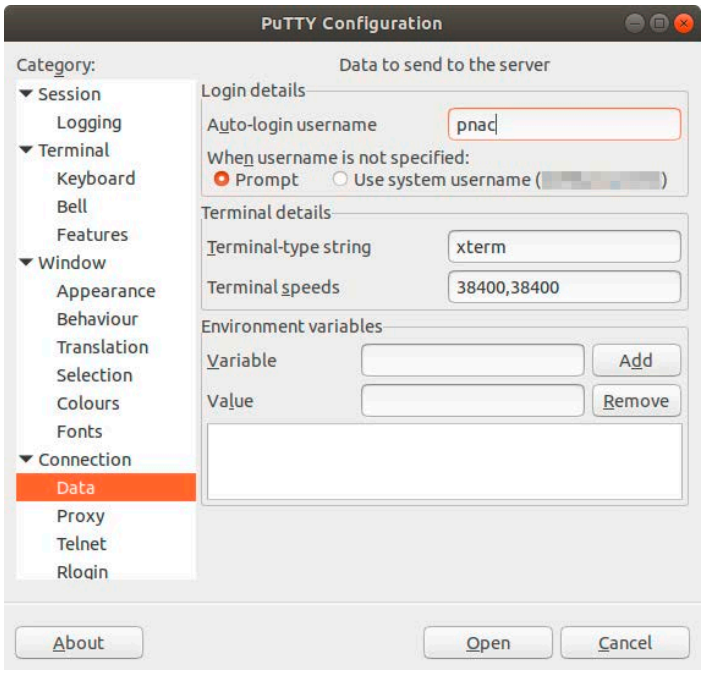


Under **Session** you can enter the IP address of the TCC2. Choose SSH connection on port 22.

For easy reuse, you can save the settings with the **Save** button.



Under **Connection -> SSH -> Auth** you can choose authentication via key file. Please browse for the key file *pnac_key.ppk* file (for PuTTY just this one key file is needed). This is the private key in the appropriate PuTTY key format.



Under **Connection -> Data** enter *pnac* as Auto-login username.

Now connect to the TCC2 by pressing the **Open** button.

A new window opens and the connection to the TCC2 is established.

```
Using username „pnac“.
Authenticating with public key „imported-openssh-key“

No password is set for 802.1X configuration.
New Password:
Retype password:
```

Since this is the first connection you are asked to set a new password. This password must be retyped. If the entries mismatch, the complete password dialog will be repeated.

You can now continue with chapter „Configuring 802.1X“.

SSH connection with the command line tool

For the command line SSH the options are entered as arguments. The call must be as follows.

```
$ ssh -i identity_file user@hostname
```

The **-i** option is followed by the path of the key file *pnac_key*.

Note that this is not the file *pnac_key.ppk* which was used with PuTTY, but the file without file extension. It is the same key but in another file format.

The public key *pnac_key.pub* must reside in the same directory as the private key *pnac_key*.

The user is **pnac** and the hostname is the IP address of the TCC2. An example call of SSH might look like this:

```
$ ssh -i pnac_key pnac@254.169.17.31

No password is set for 802.1X configuration.
New Password:
Retype password:

Welcome to the 802.1X configuration of the TCC2!
Available commands:
  p - Print the current 802.1X configuration
  c - Step-by-step 802.1X configuration
  r - Remove and deactivate the current 802.1X configuration
  d - Date and time settings
  w - Change the current password
  q - Quit this setup without changing the 802.1X configuration
Command:
```

The connection to the TCC2 is now established. Since this is the first connection, you are asked to set a new password.

You can now continue with chapter „Configuring 802.1X“.

The SSH implementation might warn about the file permissions of the key. If that occurs, the connection might not be established. Some SSH implementations need the key file to not be writable by anyone but the owner of the file. To fix this error change the mode of the file to 600.

Transferring files to the TCC2

During the process of configuring 802.1X you will be asked to upload files (keys, certificates) to the TCC2. At that point you need to upload files using an SCP client tool (as mentioned above). Linux comes with a command line SCP client preinstalled. For Windows we recommend using PuTTY's PSCP (https://www.putty.org/) since it has the same options and arguments as the Linux version. The call is similar to the SSH call earlier.

```
$ scp -i identity_file file user@hostname:
```

The **-i** option is followed by the path of the key file *pnac-ft_key*.

Note that this file is different from the file used for the SSH connection. By using different keys, the TCC2 can differentiate between the option of uploading a file and the option of configuring 802.1X. The file argument is the path to the file to be uploaded. The username is **pnac** and the hostname is the IP address of the TCC2.

The public key *pnac-ft_key.pub* must reside in the same directory as the private key *pnac_ft-key*.

The colon is normally followed by the path on the remote machine. But in this case, the TCC2 as the server is configured to redirect the file upload to the desired directory. So no path needs to be mentioned here

PuTTY PSCP tool understands the same options and arguments, but the option **-scp** is needed.

```
$ pscp.exe -scp -i identity_file file user@hostname:
```

Since PuTTY PSCP also uses another key file format the **-i** option needs to be followed by the path of the key file *pnac-ft_key.ppk*.

Example

During configuration you are asked to upload a certificate authority list.

```
Now upload a Certificate Authority (CA) list. After successful upload enter
the filename here.
Filename: _
```

To provide this file on the TCC2 use a **separate window or terminal for the file upload** and keep the SSH session open. A successful file upload by SCP for the file might look like this.

```
$ scp -i pnac-ft_key ca.pem pnac@169.254.17.31:
Sink: C0644 1757 ca.pem                    100%   1757   604.0KB/s   00:00
ca.pem
```

Afterwards, in the SSH session enter the filename of the file just uploaded and hit enter.

```
Now upload a Certificate Authority (CA) list. After successful upload enter
the filename here.
Filename: ca.pem
```

Configuring 802.1X

Setting your password

On your first SSH connection you will be asked to set a password for subsequent connections. The password characters you enter will not be echoed, so it won't be readable on the screen.

```
No password is set for 802.1X configuration.
New Password:
Retype password: _
```

Make sure you choose a strong password with a reasonable length and characters from different categories like numbers, small letters, capital letters, special characters.

This password must be retyped. If the entries mismatch, the complete password dialog will be repeated.

On subsequent connections you will be asked to enter your password. Note that you will still need to authenticate with the key file as described.

```
Please enter your password.
Password: _
```

After the password dialogue you get several options concerning the configuration of 802.1X.

```
Welcome to the 802.1X configuration of the TCC2!
Available commands:
  p - Print the current 802.1X configuration
  c - Step-by-step 802.1X configuration
  r - Remove and deactivate the current 802.1X configuration
  d - Date and time settings
  w - Change the current password
  q - Quit this setup without changing the 802.1X configuration
Command: _
```

To change the password, you can use the **w** command.

```
Command: w
New Password:
Retype Password: _
```

The other commands are explained in the following chapters of this document.

Information on password and 802.1X configuration in case of a factory reset:

If a factory reset of the TCC2 is performed in the Control Cockpit, the password and the 802.1X configuration will not be removed.

If a factory reset of the TCC2 is performed by pressing the reset button on the device itself for 5 seconds, the password and the 802.1X configuration will be erased.

Setting the system time

Certificates have a validity period. Therefore, it is **crucial for the TCC2 to have a correct system time**. The TCC2 is equipped with a buffered RTC (real time clock), so the time will also be valid even if the TCC2 is not powered for a few days. With the **d** command you can set the system time. We highly recommend checking the system time as the first step of the configuration to make sure this will not lead to a problem later in the process.

```
Current date and time is:
Tue Jul  9 06:06:44 UTC 2019
Do you want to change the date and time? [Y/n]: y
Year (e.g. 2019): 2019
Month (1-12): 11
Day (1-31): 1
Hour (0-23): 12
Minute (0-59): 34

Current date and time is:
Fri Nov  1 12:34:00 UTC 2019
```

Step-by-step configuration

The step-by-step configuration will guide you through the setup of 802.1X. The TCC2 supports two authentication methods: EAP-TLS and EAP-PEAPv0/EAP-MSCHAPv2.

EAP-TLS

For the EAP-TLS authentication method network clients need a client certificate and private key as well as a certificate authority list with trusted certificates which has signed the client certificate. These files must be prepared using a PKI (public key infrastructure). The TCC2 supports certificates as per X.509 standard. PFX or PKCS#12 are currently not supported and must be converted before using them with the TCC2.

```
Welcome to the 802.1X configuration of the TCC2!
  Available commands:
  p - Prints the current 802.1X configuration.
  c - Step-by-step 802.1X configuration.
  r - Removes and deactivates the current 802.1X configuration.
  d - Set date and time.
  w - Change the current password.
  q - Quits this setup without changing the 802.1X configuration.
Command: c

Please choose the authentication method.
Possible settings are:
  1 - EAP-TLS
  2 - EAP-PEAP (PEAPv0/EAP-MSCHAPv2)
Method: 1
```

After choosing EAP-TLS as the authentication method you will be asked for the following information:

1. Username / identity of the client
2. Certificate authority list (file)
3. Client certificate (file)
4. Client private key (file)

An example configuration might look like this.

```
Please enter your identity: user@example.org

Now upload a Certificate Authority (CA) list. After successful upload enter
the filename here.
Filename: ca.pem
Verifying Certificate Authority (CA) list...
issuer= /C=FR/ST=Radius/L=Somewhere/O=Example
Inc./emailAddress=admin@example.org/CN=Example Certificate Authority
Certificate Authority (CA) list is valid!

Now upload your client certificate. After successful upload enter the
filename here.
Filename: client.pem
Verifying client certificate...
/home/pnac/tmp/client.pem: OK
Client certificate is valid!

Now upload your private key file. After successful upload enter the
filename here.
Filename: client.key
Is the key file password protected? [Y/n]:
Please enter the password for the key.
Password:
Retype password:
Verifying key file...
RSA key ok
Key file is valid!

802.1X successfully configured with „EAP-TLS“ for user user@example.org.
The new configuration will be activated after a reboot.
```

Sometimes the private key and the client certificate are combined in a single file. If that is the case, just upload that file once when asked for the client certificate and reuse the same filename in the step asking for the client key.

EAP-PEAPv0/MSCHAPv2

For the EAP-PEAP authentication method, network clients need a certificate authority list with trusted certificates. The TCC2 supports certificates as per X.509 standard. PFX or PKCS#12 is currently not supported and must be converted before using them with the TCC2. The client will later authenticate against the server with credentials.

```
Welcome to the 802.1X configuration!
  Available commands:
  p - Prints the current 802.1X configuration.
  c - Step-by-step 802.1X configuration.
  r - Removes and deactivates the current 802.1X configuration.
  d - Set date and time.
  w - Change the current password.
  q - Quits this setup without changing the 802.1X configuration.
Command: c

Please choose the authentication method.
Possible settings are:
  1 - EAP-TLS
  2 - EAP-PEAP (PEAPv0/EAP-MSCHAPv2)
Method: 2
```

After choosing EAP-PEAP as the authentication method you will be asked for the following information:

1. Username / identity of the client
2. Password of the client
3. Client authority list (file)

An example configuration might look like this.

```
Please enter your username: johndoe

Now upload a Certificate Authority (CA) list. After successful upload enter
the filename here.
Filename: ca.pem
Verifying Certificate Authority (CA) list...
issuer= /C=FR/ST=Radius/L=Somewhere/O=Example
Inc./emailAddress=admin@example.org/CN=Example Certificate Authority
Certificate Authority (CA) list is valid!

Please enter the password for username „johndoe“
Password:
Retype password:

802.1X successfully configured with „EAP-PEAP“ for user johndoe.
The new configuration will be activated after a reboot.
```

Removing the 802.1X configuration

If you wish to remove the configuration and all according files from the TCC2, you can use the **r** command. There is no way to restore the information and files afterwards. Note that the **r** command will not remove your password for the SSH connection.

```
Welcome to the 802.1X configuration of the TCC2!
  Available commands:
  p - Prints the current 802.1X configuration.
  c - Step-by-step 802.1X configuration.
  r - Removes and deactivates the current 802.1X configuration.
  d - Set date and time.
  w - Change the current password.
  q - Quits this setup without changing the 802.1X configuration.
Command: r

This will remove your 802.1X configuration and delete all certificates and
keys.
Are you sure you want to do that? [y/N]: y
The 802.1X configuration along with its according files and certificates
has been removed. It will be deactivated after a reboot.
```

Information on password and 802.1X configuration in case of a factory reset:

If a factory reset of the TCC2 is performed in the Control Cockpit, the password and the 802.1X configuration will not be removed.

If a factory reset of the TCC2 is performed by pressing the reset button on the device itself for 5 seconds, the password and the 802.1X configuration will be erased.