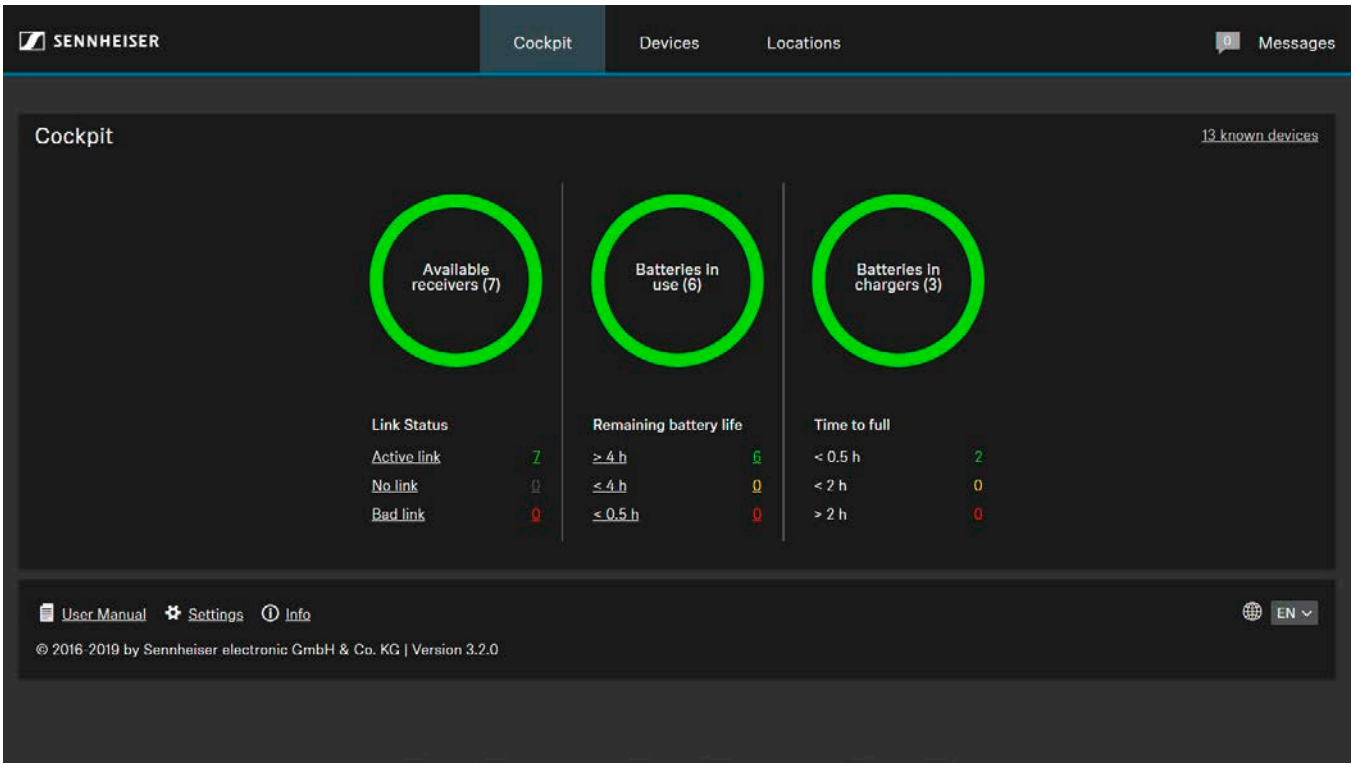


Sennheiser Control Cockpit

Running Sennheiser Control Cockpit over HTTPS

Sennheiser electronic GmbH & Co. KG

Am Labor 1, 30900 Wedemark, Germany, www.sennheiser.com
AN 1259 v1.1 | 05/21

SENNHEISER

Contents

Running Sennheiser Control Cockpit over HTTPS

v1.1 | 05/2021

Disclaimer

You can use SSL to secure parts of the communication with Sennheiser Control Cockpit service to the client‘s web browser.

SSL/TLS configuration is outside the scope of Sennheiser‘s support and the information of this document is provided without warranty of any kind, whether expressed or implied.

To ensure the correct installation of security certificates, it is highly recommended to consult the IT Security Manager responsible for the Public Key Infrastructure (PKI) within your company and the provider of the respective certificate.

Introduction

Since the Sennheiser Control Cockpit is a web application, there is communication between the client‘s web browser and the Control Cockpit application running on a server. This server and client might be the same machine, but in most cases they are different machines.

The unsecured communication running through a network can be intercepted or manipulated, user names or passwords might be intercepted by a third party. Therefore, Sennheiser strongly advises to use the Sennheiser Control Cockpit over HTTPS.

This additional security might result in a slower performance. As with all security measures, it will not guarantee security, but raises the barrier to attacks significantly.

Additionally, the involved systems should always be up to date and unique, strong passwords should be used. Furthermore, common good practices for increasing network security should be applied.

General Information

Certificate signature types

Essentially, HTTPS is a certificate containing a public key of an asymmetric key pair and the corresponding private key that is stored in a protected data space. This certificate is kept within the Microsoft Windows Certificate Store.

You can either get an official certificate, signed by a trusted Certificate Authority (CA) or create your own self-signed certificate.

Authority-signed certificate (recommended)

A certificate that has been given out by an internal or public Certificate Authority can be used for production servers. Browsers and clients will trust the certificate.

- If you are running your own Public Key Infrastructure (PKI) within your company, you can sign the Sennheiser Control Cockpit HTTPS certificate from this internal Certificate Authority. Company owned clients and web browsers will trust this certificate issuer. This is typically applied for encrypted services which are only meant for company internal usage. Please contact the operator of your Public Key Infrastructure for further assistance.
- You can also purchase a signed certificate from a public Certificate Authority. Common web browsers and clients will trust those certificate issuers. This should typically apply if the Sennheiser Control Cockpit can be accessed from not centrally managed clients, untrusted networks or the Internet.

Self-signed certificate (optional)

A self-signed certificate should only be used for testing purposes or internal servers. As the name implies, these certificates have not been signed by a public, well-known Certificate Authority. Therefore, the identity of the server using them is not trusted by clients.

Setup overview for HTTPS run

To set up the Sennheiser Control Cockpit for HTTPS the following main steps have to be made:

1. „Create or request a certificate“
2. „Reserve the domain and its port for HTTPS“
3. „Bind the certificate to the connection“
4. „Configure the Control Cockpit to use HTTPS“
5. „Restart the Control Cockpit and log on“

„Optional: Open a port in your firewall and trust the certificate on the client(s)“

Requirements

The following requirements must be fulfilled for the next steps:

- Sennheiser Control Cockpit Software version 3.3.0 or higher is installed to the default location with default settings
- The machine intended for the application is running at least the operating system Microsoft Windows 10 or Microsoft Windows Server 2019
- Accessible administrative rights for the machine

Step-by-step Guide

In this document you will find the following paragraph formats to help you read and understand the guide:

This is a note

▷ This is a task

✓ This is an intermediate result

☑ **This is a final result**

⇨ This is the further necessary step

Running Sennheiser Control Cockpit over HTTPS

1. Create or request a certificate

Depending on the desired certificate type, please follow the instructions in the respective chapter:

„Create an authority-signed certificate“

„Create a self-signed certificate“

For production servers it is strongly recommended to use a certificate that has been issued by an internal or public Certificate Authority.

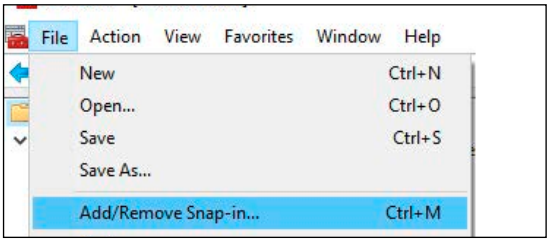
Create an authority-signed certificate

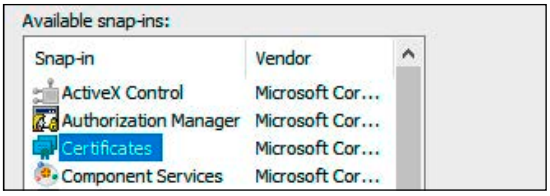
In order to use authority-signed certificate you have to create a Certificate Signing Request (CSR) and send it to the Certificate Authority. Depending on your Certificate Authority there might be a manual, script or even application to create such a request.

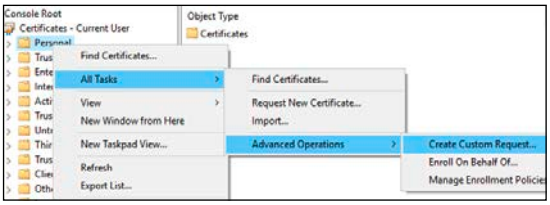
Due to the dependency on the Certificate Authority and your network setup, please refer to the Certificate Authority or your IT department for further assistance.

To create a Certificate Signing Request:

- ▷ Start the `Microsoft Management Console` by clicking the Windows logo in your task bar.
- ▷ Type `mmc.exe` and run this command as an administrator.
- ▷ Add the `Certificates` Snap-In via `File\ Add/Remove Snap-in...`.
- ▷ Choose the Certificates for the local computer.
- ▷ Select the `Personal` node of the certificates inside the new tree view in the left panel of the `Microsoft Management Console`.
- ▷ With a right click select `All Tasks` and then `Advanced Operations` and click `Create Custom Request`.
- ▷ Choose to `Proceed without enrollment policy`, unless otherwise noted by your administrator.

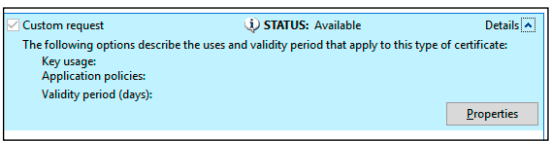


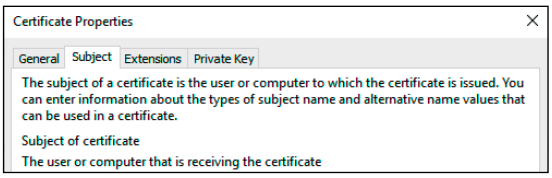




In order to match specific requirements, please refer to the Certificate Authority or your IT department before taking the next steps.

- ▷ Click on:
  - `Next`, if no specific requirements are needed (default settings will be applied)
  - `Properties` under the dropdown `Details` to meet your specific requirements within the tabs:
    - `General`
    - `Subject`
    - `Extensions`
    - `Private Key`

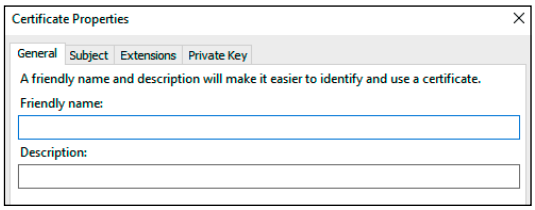




To meet your specific requirements you will find the following attributes under the respective tabs:

General

For the field „Friendly name“ it is recommended to use `SennheiserControlCockpitCertificate`. Any further settings depend on your chosen Certificate Authority.

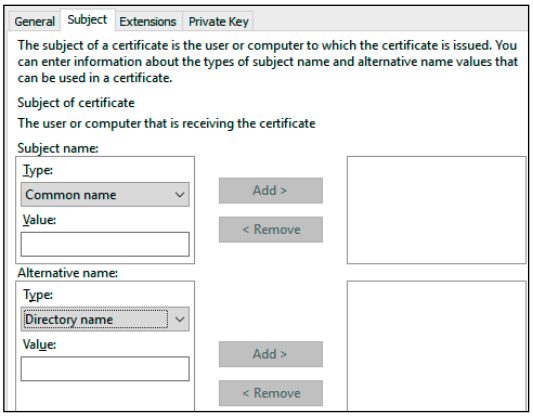


Tab „General“

Subject

In the `Subject` tab you have the `Subject name` box containing the following fields:

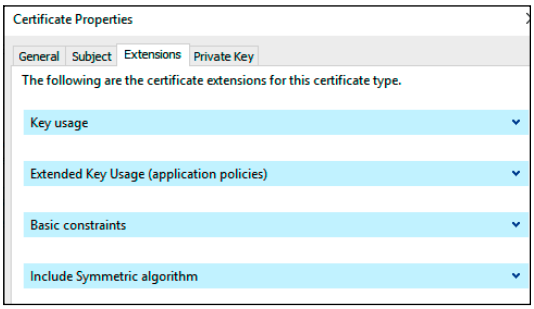
- `Common Name` (CN) - This is the server‘s fully qualified domain name or the IP address or short name of an internal server.
- `Organization` (O) - This is the name of your company or organization.
- `Organizational Unit` (OU) - The department or unit of your company, e.g.: Information Technology.
- `Locality` (L) - The city where your organization is located or has its legal location.
- `State` (S) - The name of the state or province your organization is based. Please do not use an abbreviation but the full name.
- `Country` (C) - This is the country you are located in, written in the two letter ISO country code. For example, these codes are `US` for United States, `GB` for Great Britain (UK), `DE` for Germany, `FR` for France or `ES` for Spain.



Tab „Subject“

In the `Alternative name` box, the following field is of particular interest:

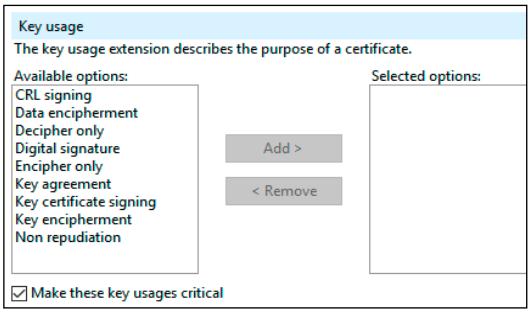
- `DNS` - This field allows giving all different names of you server, e.g. „`myHostname`“, „`127.0.0.1`“, „`myHostname.internal.myCompany.com`“. Newer browser versions rely on this so called Subject Alternative Name (SAN) attribute of the certificate.



Tab „Extensions“

Extensions

If you want to widen the possible usage of the certificate, then uncheck „`Make the Extended Key Usage critical`“ within the `Extensions` tab.



Unchecking „critical key usage“

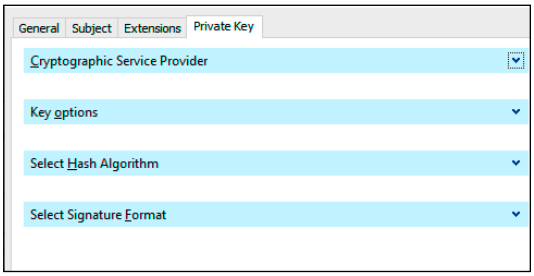
Private Key

On the `Private Key` tab you can choose some encryption options, e. g.:

- `Key Size`:
  it is recommended to use 2048 bits).
- `Provider`:
  For the choice of the Cryptographic Service Provider the default RSA should be suitable.

▷ Click on `Apply` ▸ `OK` ▸ `Next` to close the settings and to create the request file.

☑ **You have successfully created a request file** (`*.req`).



Tab „Private Key“

The generated file includes a text containing a chunk of characters between

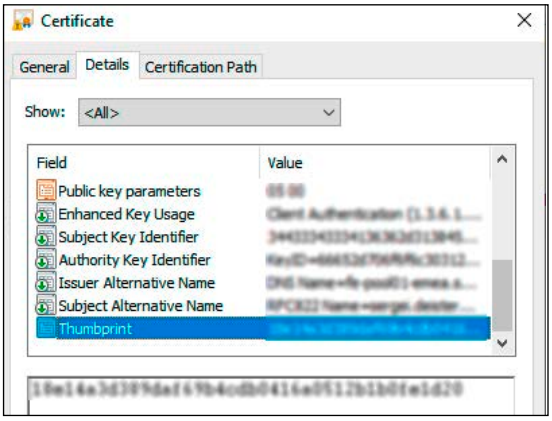
`-----BEGINN NEW CERTIFICATE REQUEST-----`

and

`-----END NEW CERTIFICATE REQUEST-----`

Example of the generated request file

- ▷ Provide the generated request file or its content to the Certificate Authority.
- ✓ You will receive a certificate from the Certificate Authority.
- ▷ Install the received certificate into the certification store `LocalMachine\My`.
- ✓ In the detailed properties of the certificate you will find a `Thumbprint`.
- ▷ Copy the Thumbprint of the certificate for the next step.
- ⇨ Next step: 2. Reserve the domain and its port for HTTPS.



Thumbprint of the certificate

Create a self-signed certificate

Depending on your network settings you will have to use a different DNS Name and/or IP. Please make sure that you are aware of additional parameters (e. g. `-KeyAlgorithm` and `-KeyLength`) to adjust the command according to your personal requirements.

For `-KeyLength` it is recommended to use at least a 2048 bit key length.

For more information about this command and its parameters, please refer to: Microsoft | Windows IT Pro Center

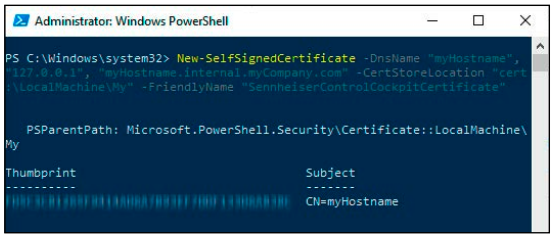
To create a self-signed certificate on a Windows 10 machine:

- ▷ Run the Windows PowerShell as administrator on the particular machine to host the Sennheiser Control Cockpit.

Store your private keys in a safe place and never disclose them. Since this certificate contains a private key, it should not leave your machine.

- ▷ Create a certificate with the following command by additinally adding your private key:

```
New-SelfSignedCertificate -DnsName
"myHostname", "127.0.0.1",
"myHostname.internal.myCompany.
com"-CertStoreLocation
"cert:\LocalMachine\My" -FriendlyName
"SennheiserControlCockpitCertificate"
```



Self-signed certificate and thumbprint

- ✓ A new Thumbprint will be given back by the reply of the command.
- ▷ Copy the Thumbprint of the certificate.
- ▷ Trust this certificate later in your browser when using a self-signed certificate.
- ☑ **You have successfully created a self-signed certificate.**
- ⇨ Next step: 2. Reserve the domain and its port for HTTPS

2. Reserve the domain and its port for HTTPS

In the following section you want to securely host the Sennheiser Control Cockpit on TCP port 443, which is the default port for HTTPS.

If you are using another port than 443, please change the port number accordingly.

Since the Sennheiser Control Cockpit is not running with administrative privileges on the machine, its URL has to be registered for non-administrator users and accounts.

▷ Run a command line (click the Windows icon in the taskbar and search for `cmd.exe`) with administrative rights and enter the following in the command line:

```
netsh http add urlacl url=https://+:443/ user=Everyone
```

Please note that the Windows system might have different names for the user groups if you are running a non-English Windows.

☑ **You have successfully reserved the domain and its port for HTTPS.**

➪ Next step: „Bind the certificate to the connection“

3. Bind the certificate to the connection

The certificate received in step 1 has to be bound to the connection of the Sennheiser Control Cockpit. To identify the certificate, its hash value has to be passed to the command. This hash is the `<<<THUMBPRINT>>>`.

To configure a port, the tool you use depends on the operating system that is running on your machine. The following tools are recommended for:

`Windows Server 2003: HttpCfg.exe` (already installed)

`Windows Vista: Netsh.exe` (already installed)

For more information about how to bind a certificate, please refer to:

Windows Communication Foundation

To bind the certificate:

▷ Alter the following command accordingly and enter it into the command line:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=<<<THUMBPRINT>>>
appid={214124cd-d05b-4309-9af9-9caa44b2b74a}
```

If the command does not work within a line, try to write the command in individual lines:

```
netsh
http
add sslcert ipport=0.0.0.0:443 certhash=<<<THUMBPRINT>>>
appid={214124cd-d05b-4309-9af9-9caa44b2b74a}
```

☑ **You have successfully bound the certificate.**

➪ Next step: „Configure the Control Cockpit to use HTTPS“

4. Configure the Control Cockpit to use HTTPS

To use the Sennheiser Control Cockpit via HTTPS and to redirect HTTP traffic to https the config file has to be extended by two additional parameters.

To configure the Control Cockpit:

▷ Open `custom.config` in a text editor under:
`C:\Users\Public\Documents\Sennheiser\Sennheiser Control Cockpit\config\custom.config`

▷ Search for the XML Tag <serviceElement>

▷ Add the two parameters `enableHttps` and `secureServerPort` as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
 <configuration>
  <SlCtrlAppConfiguration version="7">
   <serviceElement serverPort="8181"
              enableHttps="true" secureServerPort="443"/>
     ...
```

☑ **You have successfully configured the Control Cockpit to use https.**

⇨ Next step: „Restart the Control Cockpit and log on“

5. Restart the Control Cockpit and log on

▷ Restart the Sennheiser Control Cockpit and try to log on.

If you have any issues accessing the website, proceed with the optional step: „Optional: Open a port in your firewall and trust the certificate on the client(s)“

☑ **You are successfully runnnig Sennheiser Control Cockpit over HTTPS.**

Optional: Open a port in your firewall and trust the certificate on the client(s)

If you are accessing from a remote machine to the server running the Sennheiser Control Cockpit, you might have to open the incoming port 443 on the server‘s firewall.

Exported and distributed certificates should never contain a Private Key! For managing your certificate store you can use the `Microsoft Management Console` that was also used in step 1: “Create an authority-signed certificate“.

To open a port when using the Windows Defender Firewall:

▷ copy the `ControlCockpit WebUI` in the `Inbound Rules`

▷ rename it to `ControlCockpit Secure WebUI`

▷ change the local port to 443.

Depending on the certificate used, a warning may appear when logging in to the Sennheiser Control Cockpit website that the certificate is not secured.

To trust the certificate on the clients:

▷ Click on „Trust this certificate“ in your browser or deploy an exported version of your certificate to the `Trusted Root Certification Authorities` node of your certificate store.

☑ **You have successfully changed the port and the certificate trust settings.**

Additional Considerations

Certificates have a limited lifetime, i. e. they are valid from a certain point in time until another date. The issuer of a certificate defines its lifetime.

For Windows 10 this lifetime is typically 1 year if not otherwise specified. This means that the certificate has to be renewed after a year.

Therefore, you might want to consider setting up a Windows Domain with a Windows Certificate Service.