DeviceHub

Cloud based control software

PDF Export of the Original HTML Manual

Contents

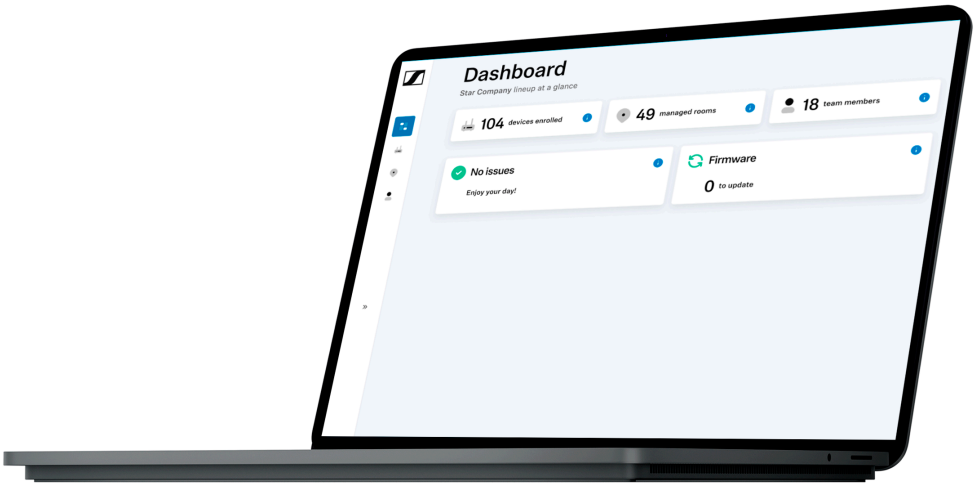
1. Preface

PDF Export of the Original HTML Manual

This PDF document is an automatic export of an interactive set of HTML manuals. Some content and interactive elements may not be included in the PDF because they cannot be displayed in this format. In addition, automatically generated page breaks may cause related content to be slightly shifted. We can therefore only guarantee the completeness of the information in the HTML manual and recommend using it. You can find it in the Documentation Portal at www.sennheiser.com/documentation.

2. Product Information

Information about supported devices, design, functionality, and the main features of the software at a glance.



What is Sennheiser DeviceHub?

Sennheiser DeviceHub is a cloud-based platform for managing and monitoring Sennheiser AV devices across locations. It provides centralized visibility, configuration, and control from any browser, supporting both on-site and remote workflows. Designed for AV and IT professionals, DeviceHub helps maintain system reliability, streamline operations, and enable secure collaboration across distributed environments.

Access DeviceHub at https://devicehub.sennheiser.com.

Remote monitoring & control

Monitor and manage Sennheiser devices from anywhere through a single, browser-based interface. Real-time status information and diagnostics help identify and resolve issues quickly, reducing on-site visits and minimizing downtime.

Location management

Organize devices by locations, buildings, floors, and rooms to reflect your real-world setup — whether within one site or across multiple countries. This logical structure provides a clear overview of distributed environments, making it easier to locate devices, navigate large installations, and maintain visibility as your AV network expands.

Role-based access control

Enable secure, shared management across team members. Role-based permissions define user access according to responsibilities, ensuring collaboration between AV, IT, and support staff while maintaining control and accountability.

Security & compliance

The Sennheiser DeviceHub platform uses security-by-design principles, Azure-hosted identity and encryption controls, and GDPR-aligned data handling to protect user information and AV infrastructure across global regions. For details, please refer to **Security and data protection**.

Supported devices

Currently the following devices are compatible with DeviceHub:

- TeamConnect Bar S
- TeamConnect Bar M

To prepare your devices for use with DeviceHub, refer to Preparing the device for DeviceHub. For more detailed information specific to TeamConnect Bars, see the Cloud Connectivity Guide.

> **i** Please note, that it's not recommended but possible to manage and monitor these device types in DeviceHub and Control Cockpit in parallel, as they remain compatible with the on-premises tool.

> **i** Compatibility with additional existing Sennheiser products will be introduced in future updates, expanding the range of device types manageable with DeviceHub.

Specifications

Supported web browsers, minimum requirements, and recommendations for using DeviceHub effectively.

Supported web browsers for DeviceHub

- **Chromium-bases browser:** Version 132 or later (Chrome, Edge, Arc, etc.)
- **Mozilla Firefox:** Version 135 or later
- **Apple Safari:** Version 18 or later

ℹ JavaScript must be enabled for full functionality.

Recommended devices & screen size

- Optimized for desktop and laptop use;
- Mobile devices and touch screens are not supported.
- Minimum recommended screen resolution: 1280 × 982 pixels

Internet connection

- A stable internet connection is required for optimal performance.
- Performance may be affected by unreliable, slow, or restricted networks.

Plugins or extensions

- No specific browser plugins or extensions are required.
- Certain browser extensions, such as ad blockers, may interfere with some DeviceHub features. Users may need to disable these extensions to adjust device configurations.

3. User Manual

Detailed description of software navigation and configuration of enrolled Sennheiser devices.

Getting Started

Initial setup steps including registration, organization, user management, and device enrollment preparation.

Follow these steps to get started with DeviceHub and prepare your organization and devices for management.

1. Prepare your devices for DeviceHub, including network connectivity, power, and firmware checks:
    - see Preparing the device for DeviceHub.
2. Register for DeviceHub and sign in with your account:
    - see Registration (Sign-up/Sign-in).
3. Set up your organization and define basic settings such as locations or rooms:
    - see Setting up organization.
4. Invite additional users and assign appropriate roles:
    - see Inviting users to organization.
5. Enroll your devices to DeviceHub and assign them to the correct rooms of your organization:
    - see Device enrollment.

Preparing the device for DeviceHub

Ensure your device is correctly set up with the latest firmware and network configuration before enrolling it in DeviceHub for effective cloud management.

Before enrolling the device in DeviceHub, make sure that it is set up correctly. This will allow you to effectively manage and monitor the device in a cloud environment.

To prepare your device for the cloud:

- Make sure that the latest firmware image supporting cloud is installed on your device by using Sennheiser Control Cockpit, which can be downloaded here: sennheiser.com/control-cockpit.
- Connect the device to the network and power.
- Make sure your device network is configured properly for cloud connectivity.

✓ The device has been prepared.

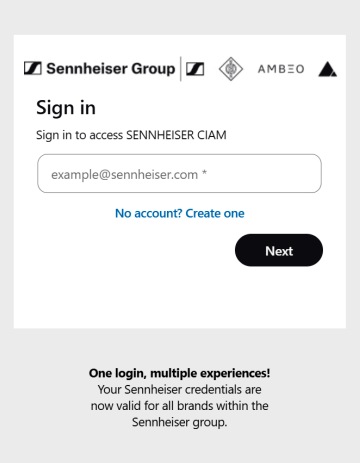
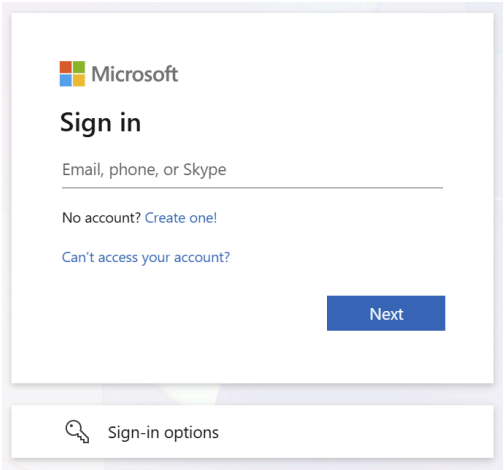
The Cloud Connectivity Guide will assist you in preparing your device for a cloud connection. Please open the document and follow the instructions before enrolling your device in the cloud.

Registration (Sign-up/Sign-in)

Learn how to sign up and sign in with a local Sennheiser account or a Microsoft account to access DeviceHub securely.

You can sign in with either a local Sennheiser account or a Microsoft account by entering your email address and password.

If a Microsoft session is already active, or after you provide valid Microsoft credentials, you are signed in and forwarded automatically.

Sennheiser Group	Global Microsoft Login
	
• Sign up or sign in with a local Sennheiser account	• Sign in with a Microsoft account
• See Sennheiser account	• See Microsoft account

Sennheiser account

Learn how to create a Sennheiser account to access DeviceHub and manage your credentials securely.

Your Sennheiser credentials are valid for all brands within the Sennheiser group.

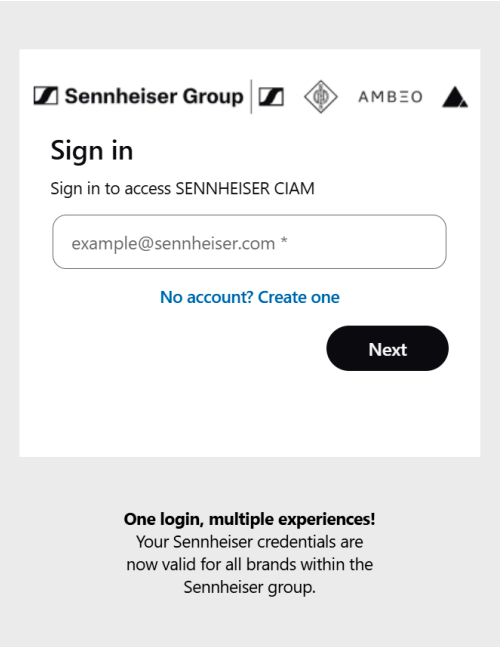
- Sign-up (Sennheiser) to create a new account services.
- Sign in (Sennheiser) with an existing account and access the application.

Sign-up (Sennheiser)

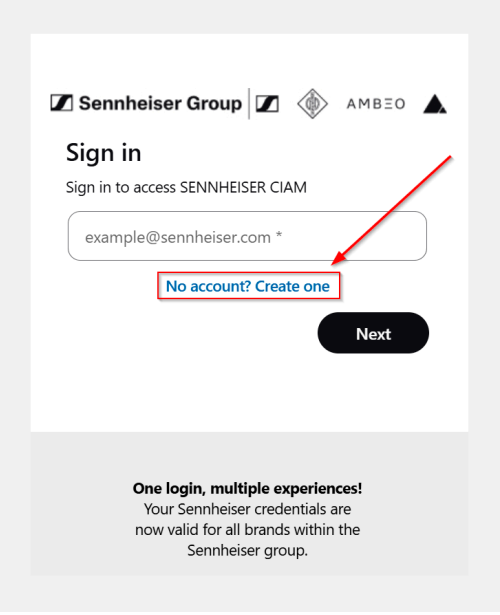
Register a new Sennheiser account in order to use DeviceHub.

To sign up:

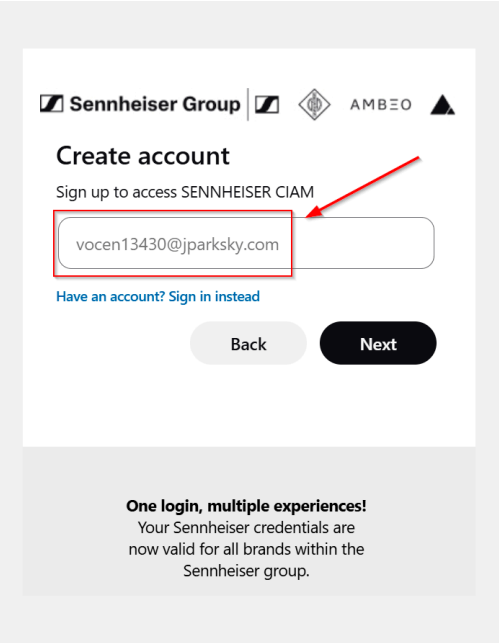
- Open the DeviceHub login page at https://devicehub.sennheiser.com/.



- Click on **No account? Create one**.

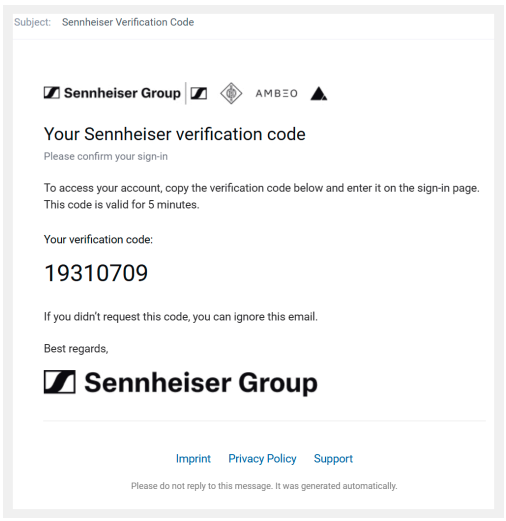


- Enter your email address in the text box.



> **i** To return to the sign-in page, click on **Have an account? Sign in instead** below the email text box.

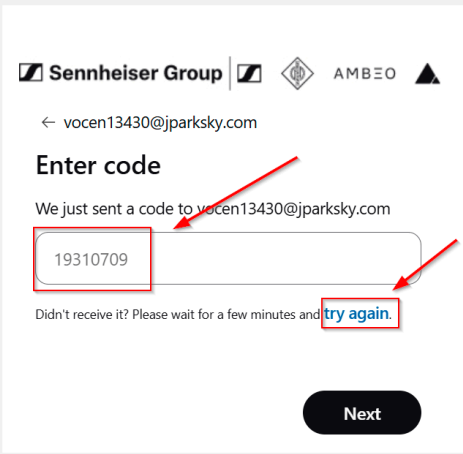
A One-Time Passcode (OTP) is sent to your email address to verify your account and looks like this:



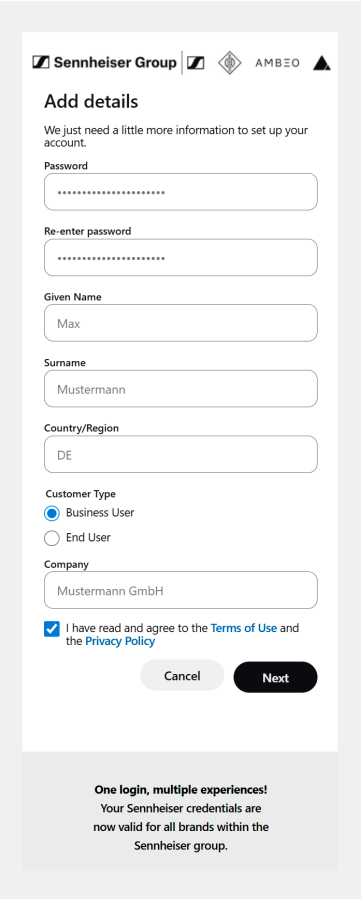
> **i** OTP codes are valid for 5 minutes only.

- Enter the OTP on the screen.

> If it takes longer than expected to receive the OTP email, a hint appears indicating that you can request a new code. Click on the link **Try again** and wait for the new OTP email to arrive in your mailbox.



- Enter your preferred password and provide all additionally required information. You must also agree to our https://www.sennheiser.com/de-de/legal/terms-of-use-ciam and Security and data protection.



> **i** Please note that the terms of use can be updated at any time during the CIAM lifecycle based on legal or infrastructure changes. By not accepting the terms of use, login access will be lost.

- Click on **Next**.

  ✓ You are logged in and redirected to the application where you started the process.

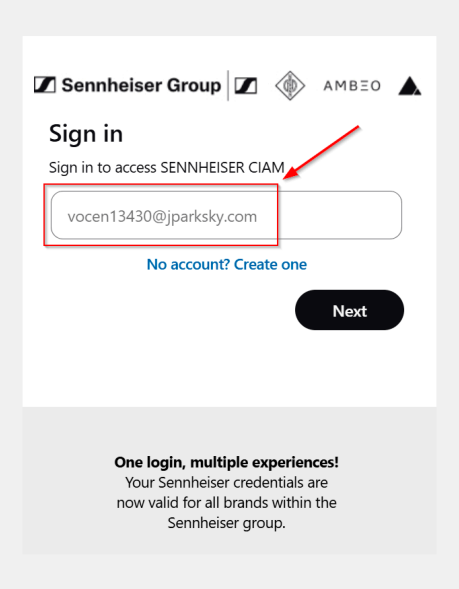
✓ You have signed up successfully.

Sign in (Sennheiser)

You can sign in with an existing Sennheiser account.

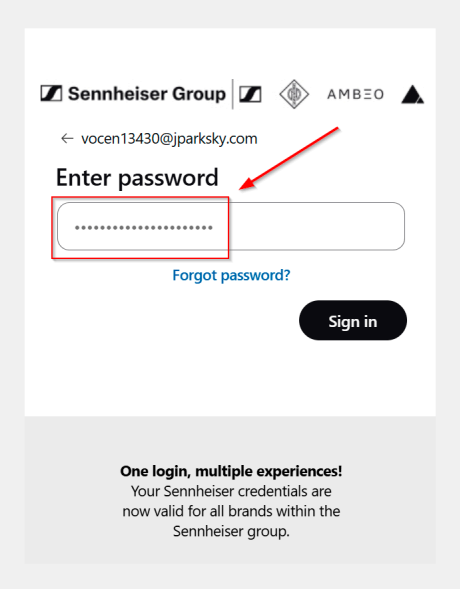
To sign in:

- Open the DeviceHub login page at https://devicehub.sennheiser.com/.
- Enter your email address in the text box.



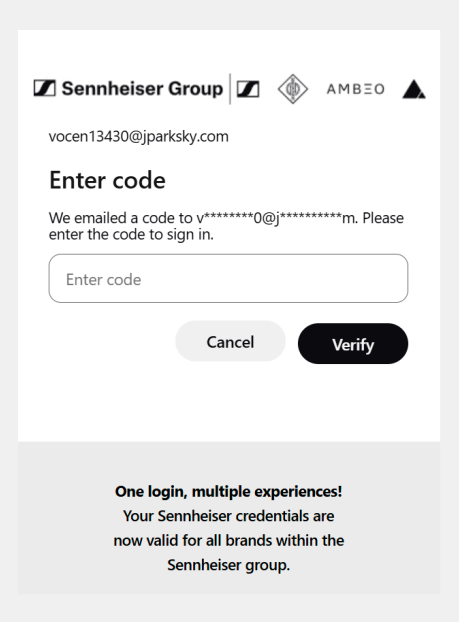
> If you can't remember your password, click the link **Forgot password?**

In some cases, you will also be asked for a One-Time Pass code (OTP). If this happens, you will see the following screen:

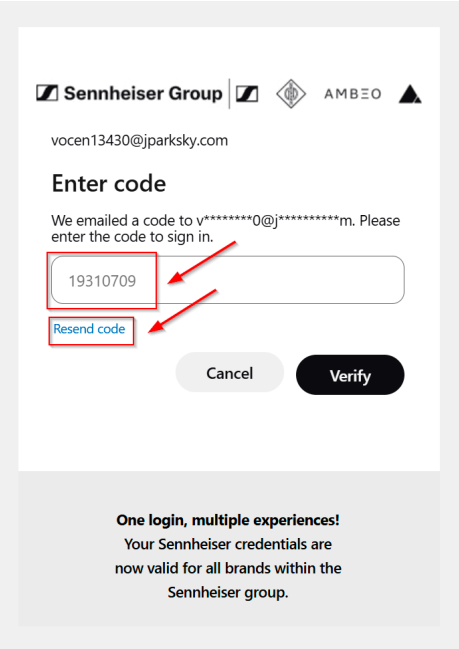


.

- Click the message **Email code to v********0@j********m**.
  - This text acts as a button and sends the OTP email to you.
- Enter the OTP code that is sent to your email for verification.



If retrieving the OTP code from your email takes longer than expected, you will see a prompt to request a new code. Click the link **Resend code** and wait for the new OTP email to arrive in your mailbox.



You have signed in successfully.

Microsoft account

You can use your existing Microsoft account to sign in to Sennheiser products.

> Please note that you cannot use a private Microsoft account for this.

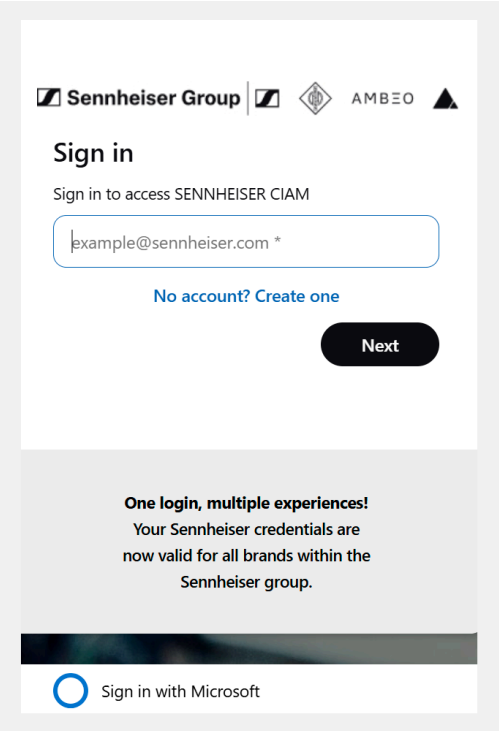
- Sign-up (Microsoft) to create a new account and use it for all future services.
- Sign in (Microsoft) to sign in with an existing account and access the application.

Sign-up (Microsoft)

Register with the Sennheiser Identity Platform using your existing Microsoft account from your customer tenant and provide the requested additional information.

To sign up:

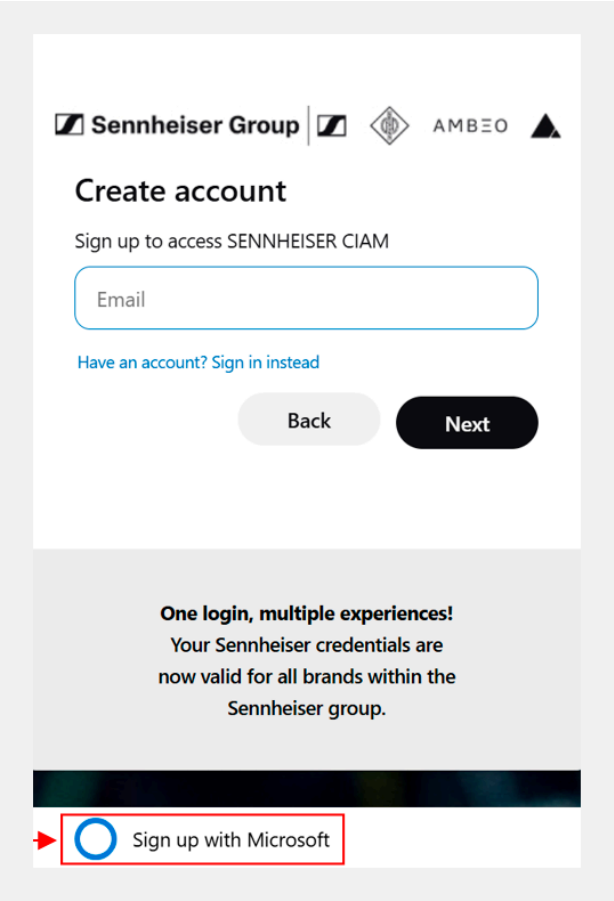
▶ Open the DeviceHub login page at https://devicehub.sennheiser.com/.



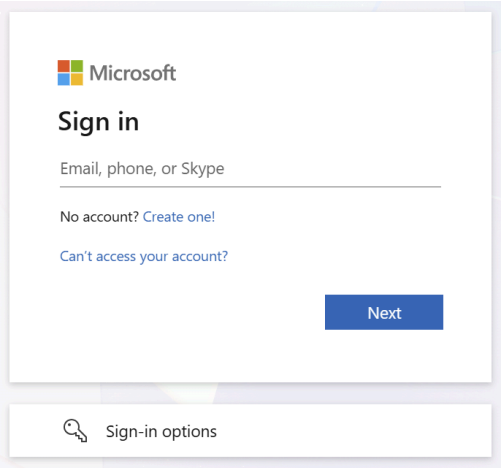
▶ Click **No account? Create one**.

✓ The Microsoft button changes from **Sign in with Microsoft** to **Sign up with Microsoft**.

You are forwarded to the common Microsoft login page.

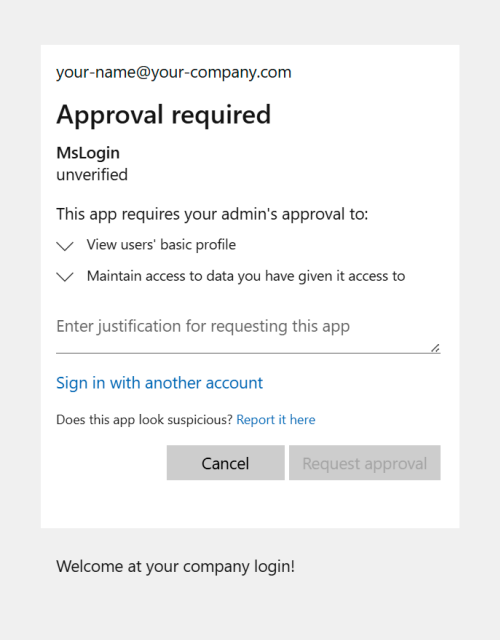


- Click on **Sign up with Microsoft** and enter your microsoft account email address.
  - After you enter your account email address, you are forwarded to your company-branded login page to enter your password. If you already have an active session for this account, you do not need to enter your password again.

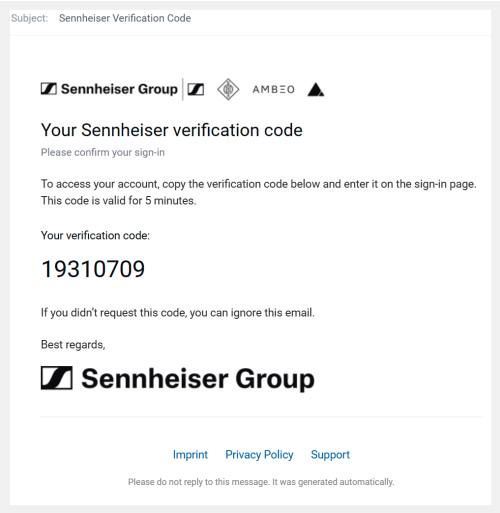


> **i** Depending on your customer tenant configuration, you may be required to complete your configured MFA challenge, such as Authenticator App, Passkeys, SMS, etc. This additional MFA depends entirely on your configuration.

> **i** If you are the first user in your company to use the Microsoft login from Sennheiser, it may happen that your administrator needs to approve the connection to Sennheiser. If this is the case, you are redirected to a page similar to this, where you are asked to enter a reason for the request (see Admin approval to enable trust between tenants).



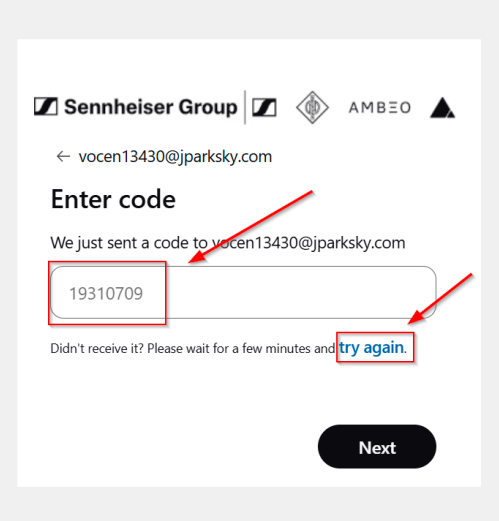
- Wait until your request has been approved by the admin.
  - Once the admin approves the request, a One-Time Passcode (OTP) is sent to your email address to verify your account and looks like this:



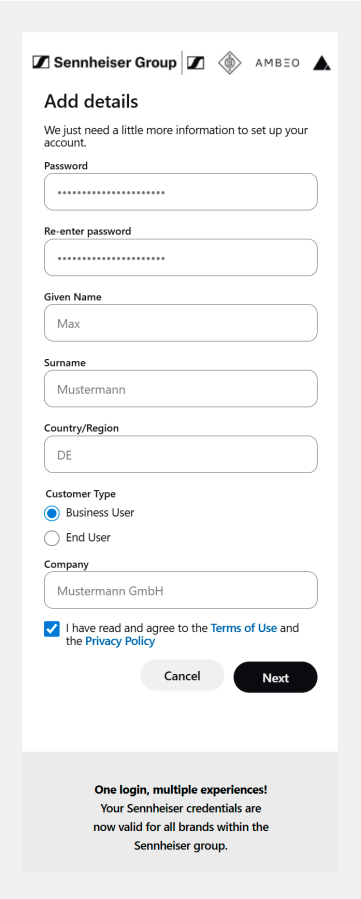
> **i** OTP codes are valid for 5 minutes only.

- Enter the OTP on the screen.

> **i** If it takes longer than expected to receive the OTP email, a hint appears indicating that you can request a new code. Click the link **Try again** and wait for the new OTP email to arrive in your mailbox.



- Enter your preferred password and provide all additional required information. You must also agree to our https://www.sennheiser.com/de-de/legal/terms-of-use-ciam and Security and data protection.



> **i** Please note that the terms of use can be updated at any time during the CIAM lifecycle based on legal or infrastructure changes. If you do not accept the terms of use, you will lose login access.

- Click **Next**.
  - You are logged in and redirected to the application where you started the process.

✓ You have signed up successfully.

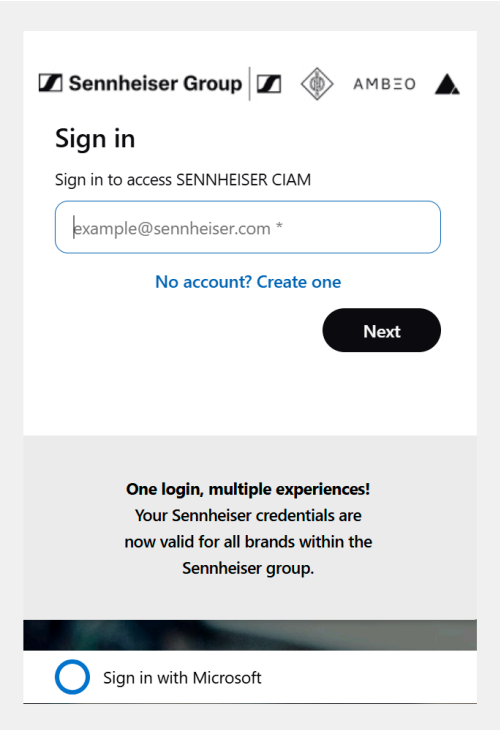
Sign in (Microsoft)

You can sign in with an existing Microsoft account.

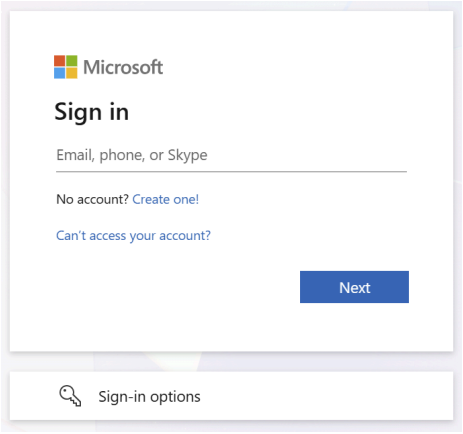
> **i** If you are the first user in your company to use Microsoft sign-in with Sennheiser, your administrator must approve the connection to Sennheiser before you can sign in with your Microsoft account. In this case, you are redirected to a page where you must enter a reason for the request (see Admin approval to enable trust between tenants).

To sign in:

- Open the DeviceHub login page: https://devicehub.sennheiser.com/.
  - ✓ A new sign in/sign-up window is displayed.



- Enter your email address and select **Sign in with Microsoft**.
  - ✓ You are redirected to the standard Microsoft sign-in page.

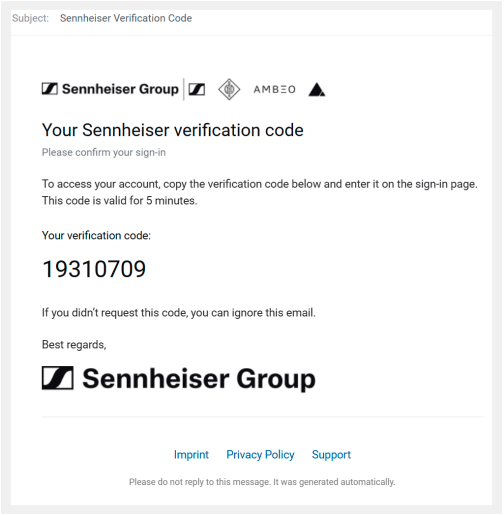


- Enter your email address again on the Microsoft sign-in page.

  After you enter your account email address, you are redirected to your company-branded login page to enter your password. If you already have an active session for this account, you may not need to enter your password again.

  > **i** Depending on your organization's tenant configuration, you may be required to complete a configured MFA challenge, such as an authenticator app, passkeys, or SMS code. The required MFA method depends entirely on your configuration.

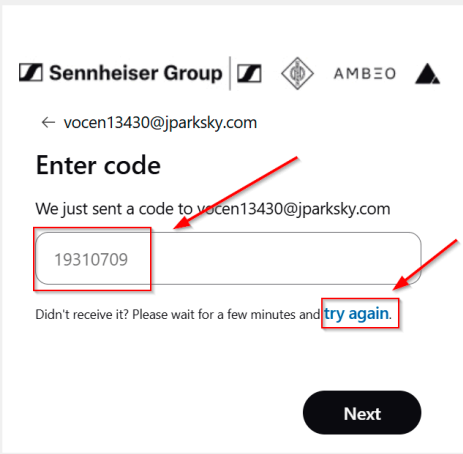
  A One-Time Passcode (OTP) is then sent to your email address to verify your account, for example:



  > **i** OTP codes are valid for 5 minutes only.

- Enter the OTP on the screen.

If it takes longer than expected to receive the OTP email, a message appears indicating that you can request a new code. Select **Try again** and wait for the new OTP email to arrive.



You have signed in successfully and can now use DeviceHub with your Microsoft account.

Admin approval to enable trust between tenants

Audience: It-admin

Administrators manage Microsoft permission consent requests and, once approved, users in the tenant can sign in to the Sennheiser screen with their Microsoft accounts.

As an admin, you are notified when there is a pending approval request. For more information about these requests, see the Microsoft documentation: Request permissions that require administrative consent.

As an admin, you can decide whether to grant or revoke permissions. After you grant the permissions, users in this tenant can use their Microsoft accounts to sign in on the Sennheiser screen.

Setting up organization

An organization serves as the central workspace within the cloud application, where both devices and team members are managed.

If you log in to DeviceHub for the first time without an invitation, you will be prompted to set up your own organization.

> **i** Each user can create only one organization with the same email address, but they may be a member of multiple organizations by accepting invitations from others. Devices, however, can only be assigned to a single organization at any given time. To move a device to a different organization, it must first be removed from its current one before being added to the new organization.

To set up an organization:

- Agree to the Terms of Use and the Privacy Policy and click **Start setup**.
- Enter the required details for your organization and your job role.
- Click **Finish setup** to complete the process.

✓ Your organization is now set up.

> **i** The name of the active organization is always displayed at the top of the side navigation bar, enabling users to easily switch between the organizations they belong to. If you are a member of multiple organizations, you can switch organizations by:
>
> - Clicking the organization name at the top of the navigation bar.
> - Selecting the desired organization from the drop-down menu.

Joining an organization by invite

Learn how to join to your organization by receiving an invitation.

To join an organization invite:

- Open the invitation email you received and click the link it contains.
  - You will be redirected to the DeviceHub account.
- Log in with your credentials or create a new Sennheiser account.
- Finalize the onboarding process and click on **Finish setup** to complete process.

You have successfully joined to your organization DeviceHub.

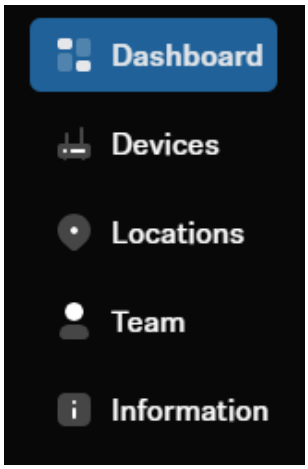
Overview

Learn about the environment of DeviceHub with a clear representation of the structure.

DeviceHub is organized into three main sections. These sections either display organization information or provide entry points to configure the application, control and manage devices, and access product information and details about supported products.

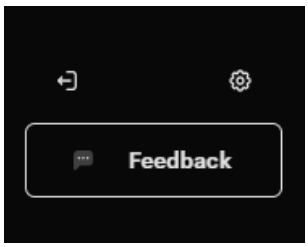
Organizational Information:

- General details about the organization



Key elements of the application:

- Dashboard: All relevant metrics of your organization and your enrolled devices
- Devices: Management of all enrolled devices
- Locations and rooms: Management of locations and rooms
- Team: Management of team members, their assigned roles and the invitation status
- Info: All important information as documentation and regulatory / legal information

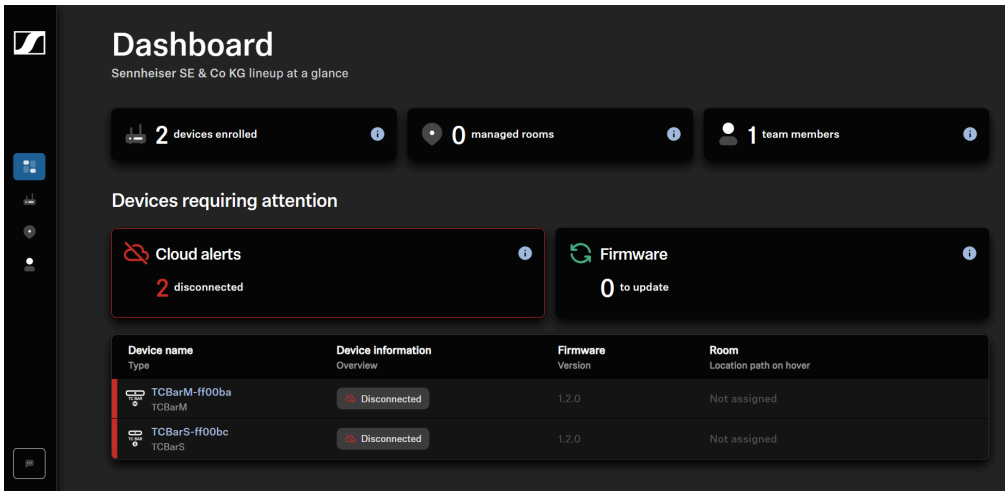


Settings and additional information:

- Log out
- Settings: Basic settings for DeviceHub
- Feedback button

Dashboard

On the dashboard page, you can see all relevant metrics of your organization and your enrolled devices.



As **organization-specific metrics** you can see the following statistics:

- **Devices enrolled:** Total number of devices registered and assigned to your organization
- **Managed rooms:** Total number of rooms with at least one assigned device in your organization
- **Team members:** Total number of users with active accounts in your organization

As **device-specific metrics** you can see the following statistics:

- **Cloud alerts:** Devices that are currently disconnected from the cloud and cannot be monitored or managed remotely
- **Device alerts:** Total number of critical alerts across all connected devices that require immediate attention
- **Warnings**: Total number of non-critical notifications across all connected devices that may indicate misconfiguration
- **Firmware:** Status of the firmware version of all devices enrolled

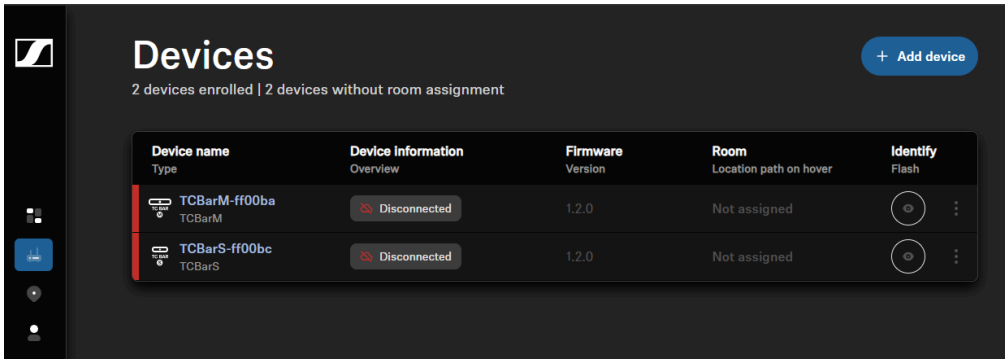
> **i** The number of enrolled devices may differ from the number shown in the list. This is because the device list only includes devices that have cloud alerts, device alerts, or warnings.

Cloud alerts, device alerts, and warnings are shown in the device list below. To filter the list, click the corresponding tile above; only one filter can be applied at a time.

> **i** From the device list you can open devices to view detailed information about any issues. Assigning devices to rooms is not available from the dashboard; you can do this only from the device list on the Device overview page.

Devices

Manage Sennheiser devices using an overview page that displays all enrolled devices, along with a detail page for configuring individual device settings.



In order to manage Sennheiser devices, you can use the following pages:

- **Device overview page** — shows all enrolled devices in a consolidated list and provides a quick summary for each device.
- **Device detail page** — focuses on a single device and displays its detailed settings and information.
- **Room page** — displays the devices assigned to a specific room.

Device overview page

On the Device overview page, the device list shows all Sennheiser devices currently enrolled to your organization. Devices in the list are sorted alphabetically by device name. In the device list the following properties of the devices are represented:

- Device name
- Device type
- Device information (shows the connection state of the device and shows potential errors and warnings)
- Firmware version
- Room assigned to the device
- Identify device

Device detail page

When you access the Device detail page for a dedicated device, you will see the device name along with the primary functions located at the top:

- mute
- reboot
- identify

Below this, a core information section displays all the essential details of the respective device immediately. This includes the following information, which may vary depending on the device:

- Room assigned to the device
- Serial number
- Firmware version

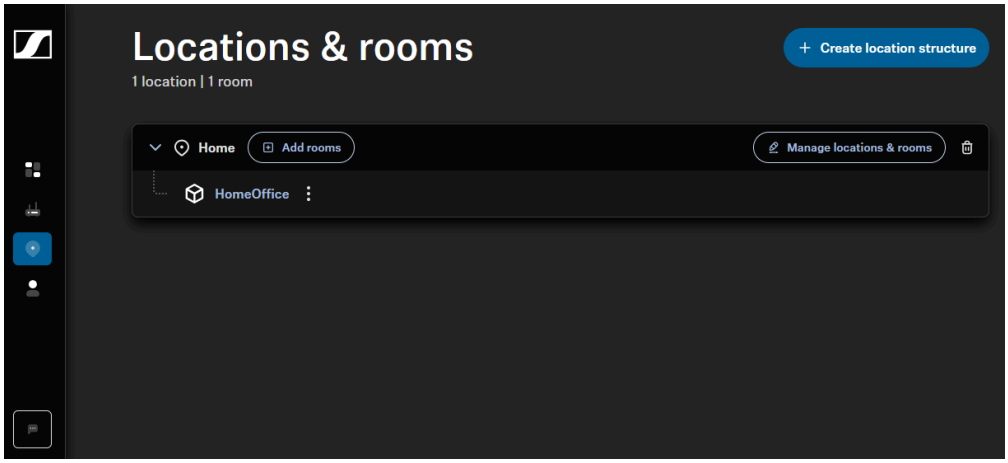
Room page

The Room Page provides a filtered list of all devices assigned to the selected room. To help clearly identify each device's location, the full location path is displayed. Devices in the list are sorted alphabetically by device name. In the device list the following properties of the devices are represented:

- Device name
- Device type
- Device information (shows the connection state of the device and shows potential errors and warnings)
- Firmware version
- Identify device

Locations and rooms

Manage the physical layout of your organization by creating, editing, and deleting locations and rooms to efficiently monitor AV device deployment.



In the Location section, you can define and organize the physical layout of your organization by creating, editing, and deleting locations and rooms. This structure helps you map the deployment of AV devices and enables efficient monitoring throughout your organization. Locations serve as high-level organizational containers, while rooms represent specific areas where enrolled devices can be assigned and managed.

> **i** The total number of locations and rooms combined is limited to 1,000. You can create up to 6 hierarchy levels of locations (excluding rooms) to reflect the complexity of your organization. A typical structure might include:
>
> - Region
> - Country
> - City
> - Street
> - Building
> - Floor

The following actions can be performed under **Locations**:

- Creating a location structure
- Deleting location structure
- Adding rooms
- Editing and deleting rooms

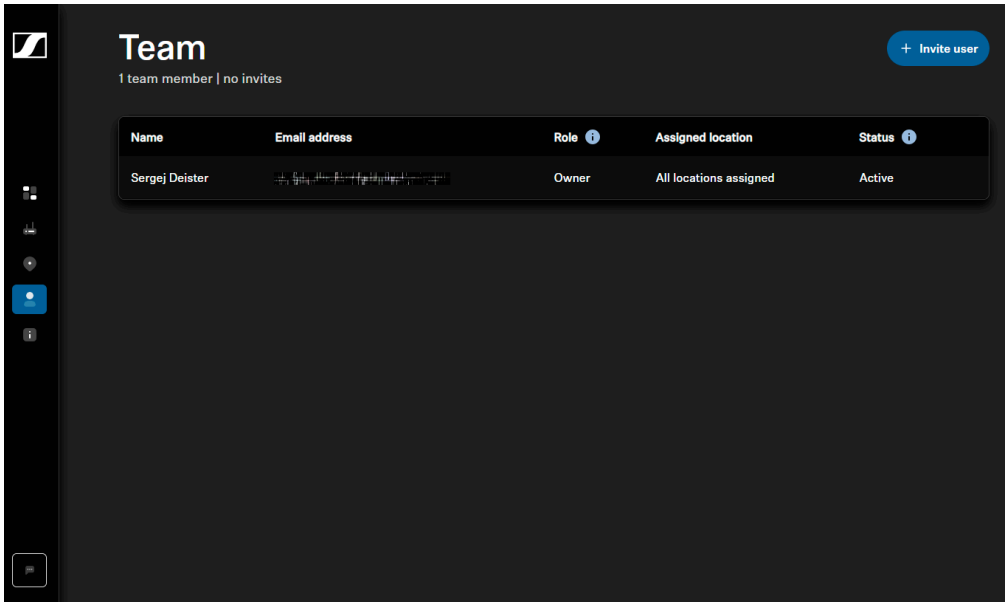
> Please note that some actions are subject to certain user rights and can only be performed with the role **Owner**. An overview of the user permissions is available in chapter Roles and permissions.

- Removing users from organization

Team

The Team section provides a comprehensive list of all users within an organization, their assigned roles and the invitation status.

Under Team, you can invite additional people to collaborate in this environment. You assign roles and can view the status of each person and manage membership.



Overview of all possible operations under Teams:

- Inviting users to organization
- Managing pending invites
- Roles and permissions
- Joining an organization by invite
- Removing users from organization

Info

Quick access to relevant topics and information about the software and the devices it operates.

Here you will find an overview of all relevant links to information on the following topics:

Documentation:

- necessary instructions for the setup and use of DeviceHub as well as instruction manuals and FAQs for supported devices.

Release Notes:

- information about the latest features, improvements, and fixed issues of the software.

Legal and compliance:

- all legally relevant information such as imprint, terms of use, privacy policy, or cookie settings.

Settings

The settings page is a centralized space where organization-, account- and personal settings can be managed based on the user's access level.

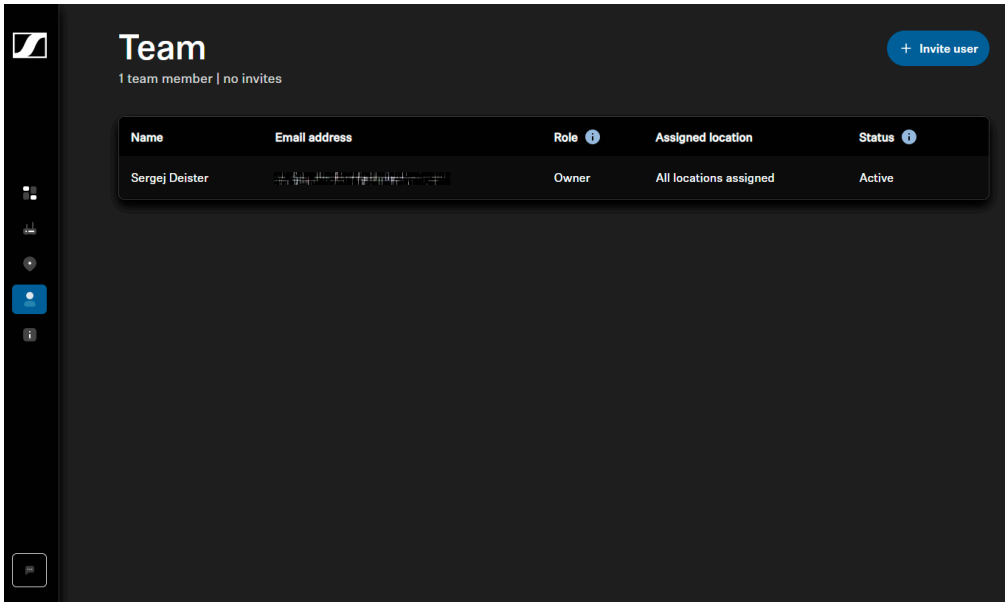
On the settings page, you can perform the following actions:

- Editing account information
- Changing your account password
- Editing organization information
- Changing display settings
- Leaving an organization
- Deleting organization
- Enabling or disabling daily device status reports

Team management

Instructions for inviting users and managing invites to ensure seamless collaboration and communication within the team.

Under Team, you can invite additional people to collaborate in this environment. You assign roles and can view the status of each person and manage membership.



Roles and permissions

User roles define default permissions that determine which actions users can perform.

In DeviceHub, different user roles can be assigned. User roles (owner and Location Admin) have predefined default permissions: owners have full administrative rights, while Location Admins have limited device-related rights.

> Please note the following rules:
>
> - Users who have created an organization are automatically assigned the owner role.
> - It is required that at least one owner is existing in an organization.
> - There can be multiple owners in one organization which all have the same rights.

Depending on the user role, different user rights apply, which are assigned by default as shown in the overview:

Types of user roles

Role	Role permission
Owner	• Can view and manage all locations • Can enroll, configure, monitor and remove devices from any location • Can add or remove users from the organization and manage user permissions • Can create and delete an organization and manage organization data. **i** An organization may have multiple owners but must have at least one.
Location Admin	• Can add and manage locations and rooms of the assigned top-location • Can view, configure and monitor all devices to the assigned top-location they were given access to **i** A Location Admin can be assigned no location during invitation or role editing; they then cannot manage devices or locations.

User roles and permissions

User rights	Owner	Location Admin
User management		
View users	✓	✓
Invite/edit users, resend/revoke invite, edit role	✓	X
Delete users	✓	X
Locations and rooms		
View locations	✓	✓ to which they are assigned to
Create/delete top locations	✓	X
Rename top locations	✓	✓
Add, edit, delete sub-locations and rooms	✓	✓ only for top-locations they are assigned to
Devices		

User rights	Owner	Location Admin
View devices	✓	✓ if assigned to their location
Enroll devices	✓	X
Configure devices	✓	✓ if assigned to their location
Assign device to room/remove room assignment	✓	X cannot see devices that are not assigned
Change room assignment	✓	✓ within location they are assigned to
Delete device	✓	X
Organization		
View organization	✓	✓
Edit organization settings	✓	X
Delete organization	✓	X
Insights		
View dashboard	✓	✓ devices assigned to their location
Filter device list	✓	✓

Inviting users to organization

Audience: Owner

Learn how to invite users to your organization by sending an email invitation through the DeviceHub application.

DeviceHub offers two different types of user roles that are tied to different level of access and permissions. All permissions apply to the organization the user is part of. For more details about user roles, see Roles and permissions.

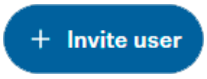
> **Only one user can be invited at a time.**
> The invitee will receive an email containing a link to join DeviceHub. They must click the link and complete the signup and onboarding process to finalize their registration with the organization. The invitation link included in the email is valid for 14 days.

> A Location Admin can still be invited when no location is assigned to them or when no locations are existing in the organization yet. Locations can be assigned to a Location Admin later. Until a Location Admin is assigned to at least one location, they do not have access to the data of any existing locations or devices.

To add a user to your organization, you need to send an invitation to their email address.

To invite a team member:

- Navigate to the section **Team**.
- Click **Invite User**.



- Enter the invitee's appropriate email address into the invite field.
- Select the appropriate user role depending on the permissions to be granted:
  - Choose **Owner** to grant the invited user access to all locations within the organization.
  - Choose **Location Admin** to select a top-level location to which the user should be granted access.
- Click on **Send Invite**.

✓ The invitation was send.

Managing pending invites

Audience: Owner

Manage pending invites by resending or revoking invitations from the Team section, which displays all unaccepted invitations.

> **i** Only an owner can invite users or manage users and their permissions within the organization.

The Team section offers an overview of all invitations that have not yet been accepted, which are indicated by the statuses "pending" or "expired." From this section, you can choose to resend or revoke invitations.

To resend an invitation:

- Locate the user with the pending or expired invitation in the user list.
- Click on the  next to the user.
- Click on **Resend Invite**.
  - The invitee will receive a new email with a refreshed invitation link, valid for another 14 days.

To revoke an invitation:

- Locate the user whose invitation you wish to revoke.
- Click on **Revoke invite**.
- Confirm to revoke the invite.
  - Revoked invitations immediately deactivate the previously sent link, and the invitee will not be notified about the revocation.

✓ The pending invites have been managed.

Managing roles and permissions

Manage roles and permissions by edit user roles, preview and change location assignments to restrict access to location and device data within the organization.

> **i** Please note that managing roles and permissions can only be done by a user who is assigned to the role **Owner**.

> **i** User roles and location assignments can be edited or changed only for active users.

Editing user role

Audience: Owner

Change a user's role between owner and Location Admin and assign location access if needed.

> **i** A user role can be changed from owner to Location Admin or from Location Admin to owner. The user is automatically notified by email when their role is changed.

> **i** A user can be assigned the Location Admin role even if no locations are currently assigned to them or if no locations exist in the organization yet. Locations can be assigned to a Location Admin later. Until a Location Admin is assigned to at least one location, they do not have access to the data of any existing locations or devices.

To assign a user role:

- In the section **Team**, click the icon button next to the user and choose **Edit user role**.
- Select the appropriate user role depending on the permissions to be granted:
  - Choose **Owner** to grant the invited user access to all locations within the organization.
  - Choose **Location Admin** to select a top-level location to which the user should be granted access.
- Click **Save**.

✓ The user role has been updated.

Previewing location assignments

Preview assigned locations for Location Admins in active, pending, or expired states.

> **i** Assigned locations can be previewed only for Location Admins who are in an active, pending, or expired state.

To preview the location assignments:

- In the **Team** section, click **Preview locations** to see the assigned locations for specific users.

✓ The location assignments are displayed.

Changing location assignments

> Location assignments can only be changed for Location Admins.

To change the location assignments:

- In the **Team** section, click the icon button next to the user and choose **Change assigned location**.
- Select the top-level locations to which the user should be granted access.

  > A Location Admin can still exist even if no locations are currently assigned to them or if no locations exist in the organization yet. Until a Location Admin is assigned to at least one location, they do not have access to the data of any existing locations or devices.

- Click **Save**.

✓ The location assignments are displayed.

Removing users from organization

Audience: Owner

You can remove users from the organization via the Team section.

> **i** When a team member is removed, they are not notified and the Sennheiser account remains unchanged.

To remove a user:

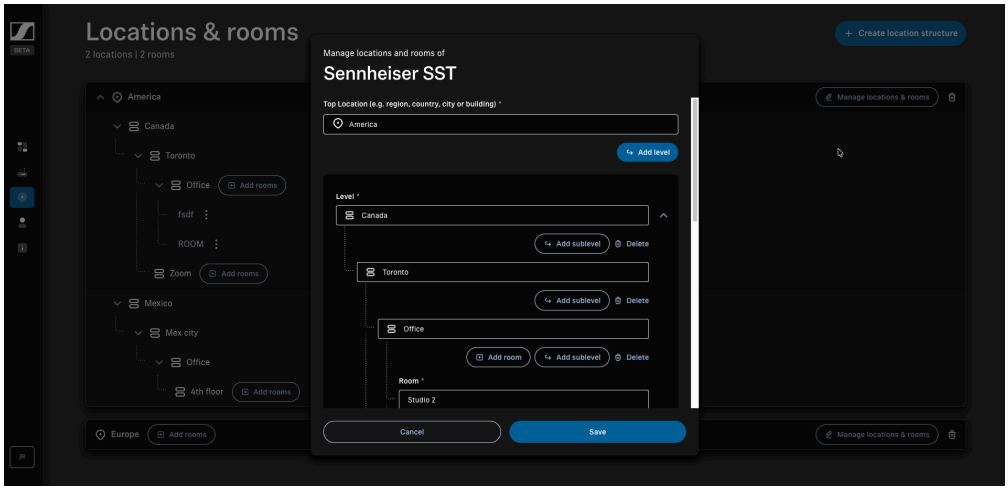
- In the section **Team**, click the bin icon next to the user who should be removed from the organization.
- Click **Remove user** in the modal to confirm the removal.
  - The removed user is immediately no longer able to access the organization.

✓ The user has been removed successfully.

Location & room management

Manage your location and room structure by adding, deleting, or renaming entries.

Locations and rooms represent the central part of the structure in DeviceHub. Here, all available devices are grouped in virtual rooms and locations, which can then be easily and quickly assigned.



Creating a location structure

Audience: Owner

Learn how to create a location structure by adding locations and rooms that reflect your organization's physical layout.

To set up a location structure, you need to add locations and rooms that reflect the physical layout of your organization. You can define multiple location structures, depending on how your organization is distributed. The first location level you create will automatically be shown as the top-level location of the location structure. Locations and rooms are sorted alphabetically within their hierarchy level.

> **i** Please note that creating and deleting a location structure can only be done by a user assigned to the **Owner** role.

To create a location structure:

- Navigate to the section **Locations**.
- Click **Create location structure**.

- Click the **+** icon next to each location input field to create a new location level or click **Add room** to create a room.
- Enter the names of your locations and rooms according to your preferred layout (e.g., **Region** > **Country** > **City** > **Building** > **Floor** > **Room**).
- Click **Save** to apply the structure and view the list of created locations and rooms.

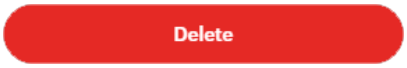
✓ A location structure has been created.

Deleting location structure

Learn how to delete a created location structure.

To delete an entire location structure:

- Navigate to the section **Locations**.
- Click the  icon next to the top-level location in the structure.
- Type the name of the location structure to confirm its deletion.
- Click on **Delete**.



The location structure has been deleted.

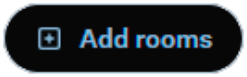
Adding rooms

Learn how to add new rooms within a created location structure.

> After adding rooms, access a room's page by clicking its name in one of the following places:
>
> - the location list,
> - the device list on the Device overview page,
> - Dashboard page, or
> - the Device detail page.

To add rooms:

- Navigate to the section **Locations**.
- Click on **Add rooms** next to the location you want to assign rooms to.



- Enter the name of your new room.
- Click on **Save**.

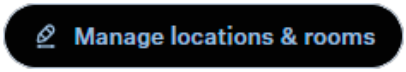
A new room has been added.

Editing and deleting rooms

Learn how to edit or delete created rooms.

To make changes to your location structure:

- Navigate to the section **Locations**.
- Under your location, click on **Manage locations & rooms**.

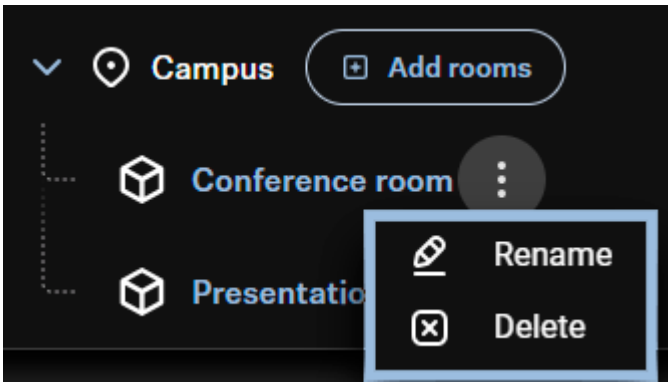


A modal opens in order to manage existing locations and rooms. Here you can add, delete, or rename both locations and rooms.

> **i** When you delete a location that has rooms assigned to it, those rooms will also be removed. If you add a new location beneath an existing location that has assigned rooms, those rooms will automatically transfer to the new lower-level location.

> **i** Different than locations, rooms can also be edited and deleted directly from the location structure list.

- Click on the ⋮ next to the corresponding room and choose the appropriate action from the drop-down menu.



- Click on **Save** or **Delete room**.

✓ The location structure has been changed.

Device enrollment

Follow the steps to enroll your device to DeviceHub, ensuring proper network connectivity and time configuration.

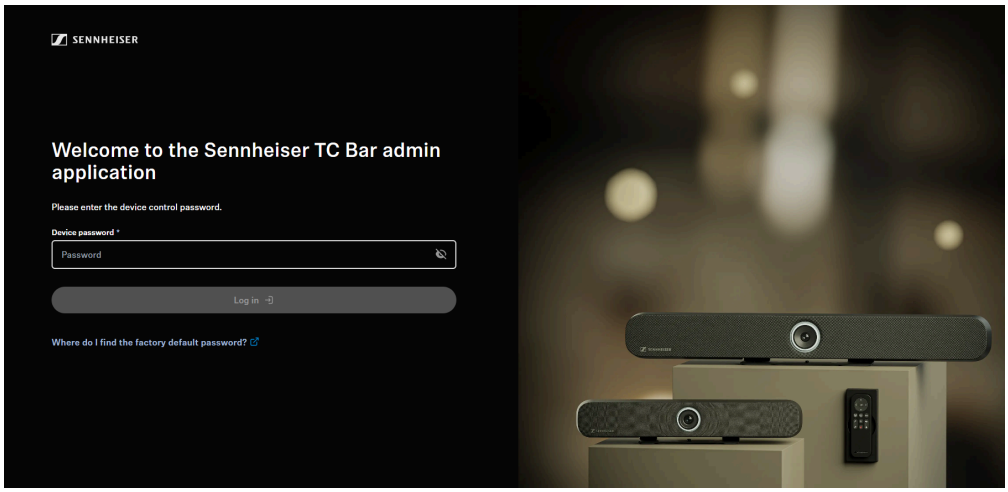
> The enrollment code is valid for 5 days and can be used for multiple devices. If the enrollment code is no longer valid, just create a new one and copy it in the Sennheiser DeviceHub by clicking **Add device** and **Copy code**.

After the device has been prepared for DeviceHub (see Preparing the device for DeviceHub), you can start the enrollment process with the following steps:

1. Running Local Web UI (LUI)
2. Configuring NTP server
3. Enabling cloud connectivity
4. Enrolling devices
5. Disenrolling devices

Running Local Web UI (LUI)

Connect and configure your device via the embedded Local Web UI.



To run the Local Web UI, perform the following steps:

1. Connect the device (e. g. TC Bar) to your network.
2. Determine the assigned IP address or hostname of the device.
3. Access the device in the browser using the IP address and initialize the device upon first use.

To access the Local Web UI:

- In your browser, navigate to the device's IP address or hostname using "https", e.g.: `https://IP-address`.

  > **i** When accessing the device via HTTPS, your browser may display a security warning. This occurs because public certificates can only be issued for fixed Internet addresses, not for local IP addresses or hostnames. The connection is encrypted and secure. If you are accessing the device within your own network, you may confirm the warning to proceed.

- Depending on your browser, click on **Advanced** and then on:
  - **Continue to localhost (unsafe)** (Microsoft Edge)
  - **Proceed to localhost (unsafe)** (Google Chrome)
  - **Accept the Risk and Continue** (Firefox)
  - or similar (other browsers).

  ✓ You now have access to the Local Web UI.

To initialize the device upon first start:

- Type in the password set in the factory state, which can be found on the back of the product label under **Default password**.

  > **i** If the device was previously initialized by another device management solution like Sennheiser Control Cockpit, the previously set password must be entered. If you cannot remember the previously set password, please check the existing configuration setup or perform a factory reset of the device.

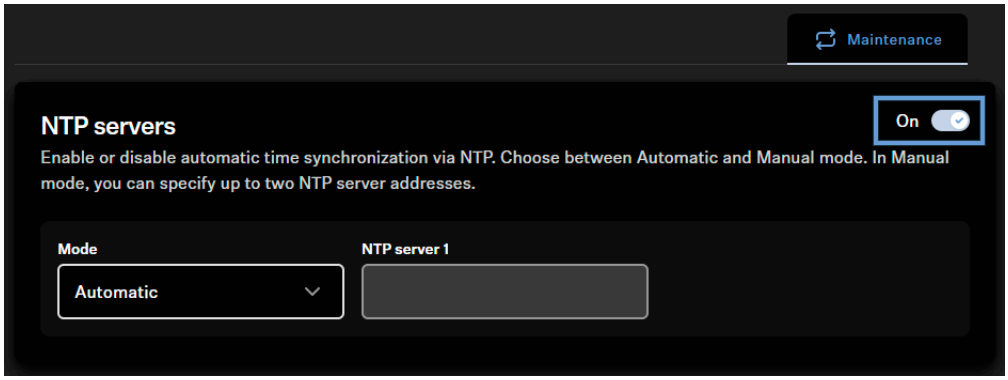
- If this device was not configured beforehand, you will be asked to set a new device password. Please enter a new device password for future configuration.

  > **i** Please note that the new password must meet the following requirements:
  > - At least ten characters
  > - At least one lowercase letter
  > - At least one uppercase letter
  > - At least one number
  > - At least one special character: !#$%&()*+,-./:;<=>?@[]^_{|}~
  > - Maximum length: 64 characters

✓ You have successfully logged into the Local Web UI.

Configuring NTP server

Enable NTP servers or use browser time temporarily.



To configure an NTP (network time protocol) server:

- In the **Local Web UI** of your device, navigate to the tab **Maintenance**.
- Set **NTP servers** to **On**.
- When activated, the system uses the NTP server provided by the DHCP server by default ("Automatic").
- If your DHCP server is not providing an NTP server or if you are using a static IP configuration, change the selection in the **NTP servers** field to “Manual” and input your NTP server. You can enter either an IP address or a DNS name.

  When configuring the time server, the device accepts any address or name provided via DHCP or entered manually, without verifying its reachability or validity. This feature allows for pre-configuration of the device for later use in a different environment. If time synchronization issues arise, please ensure that the configured server is accessible and is a valid NTP server.

  When you cannot use an NTP server, you can set the device's time to match your browser's time by clicking on "Use browser time" in the System time field.
  Please note, that this time is only kept until the next reboot/power down. To connect to the cloud after a reboot, you need to manually set the time again if not using NTP.

✓ The NTP server has been configured.

Enabling cloud connectivity

Learn how to enable the cloud connectivity for your device.

To enable the cloud connectivity:

- In the **Local Web UI** of your device, navigate to the tab **Access & Security**.
- Under **Sennheiser DeviceHub**, switch the toggle to **On**.
  - An input form for the enrollment code is displayed.

✓ The cloud connectivity has been enabled.

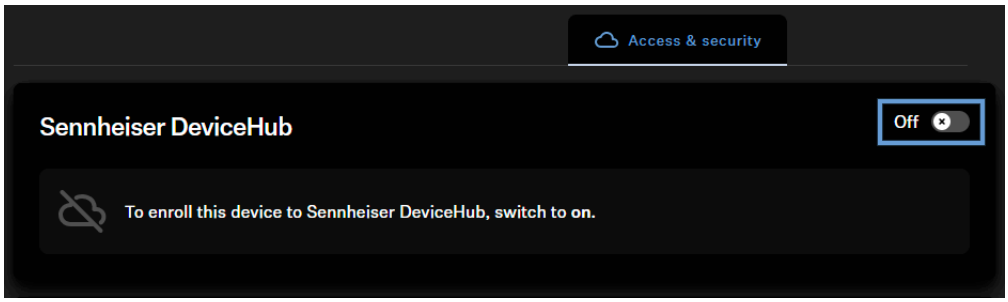
Please proceed with the next step: Enrolling devices

Enrolling devices

Audience: Owner

Learn how to enroll your device to DeviceHub.

To enroll your device:



- In DeviceHub, navigate to the section **Device**.
- Click on **Add device**.
  - An enrollment code is displayed.
- Copy the enrollment code and switch to the Local Web UI of the device.
- In the Local Web UI, navigate to the tab **Access & Security** and activate the cloud connectivity under **Sennheiser DeviceHub** (if not yet done).
  - A query form with the requested activation code is displayed.
- Enter the enrollment code in the dedicated field by pasting it.
- Click on **Enroll device**.
  - Once completed, Sennheiser DeviceHub will show the enrolled device(s) in the device list.

✓ The devices have been enrolled.

Disenrolling devices

Audience: Owner

Remove a device securely from DeviceHub to disconnect it from the organization and delete all device-related information in the IoT hub.

When a device is no longer in use or is temporarily stored, for example during a room renovation, you should remove it from your DeviceHub account to keep your device list clean and up to date. Each device can only be enrolled in one organization at a time. If you want to use a device in a new organization, you must first disenroll it from the previous organization.

To disenroll your device:

- In DeviceHub, navigate to the Devices page.
- On the device you want to disenroll, click the three dots and then click **Disenroll device**.
- Confirm the disenrollment.

  > **i** Remember to disable the cloud connectivity on the device's LUI to complete the disenrollment.

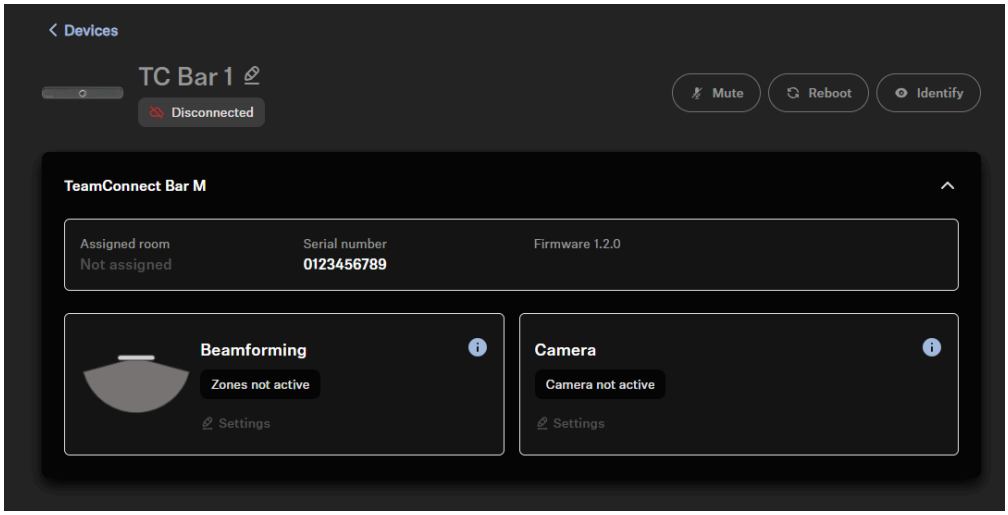
  ✓ The disenrollment starts in the background and the device shows the status **disenrolling**.

  > **i** When the disenrollment is completed successfully, the device is removed from the DeviceHub account and a success toast confirms this. If the disenrollment fails, the device appears again in the list (in its previous state) and an error message indicates the failure.

✓ The device has been disenrolled.

Device control

Configure and control devices directly using the device's familiar LUI interface in DeviceHub.



DeviceHub supports direct control via the supplied LUI interface of each individual device. Therefore, you can directly operate all functions provided in the device's LUI from DeviceHub.

Depending on the device used, please navigate to the corresponding documentation to learn about the supported features:

- TeamConnect Bar

Monitoring devices

DeviceHub provides a central Dashboard to monitor all connected devices within an organization.

By navigating to the Dashboard page, you can see all relevant information about your organization and its devices, depending on your level of access.

The following organizational information is provided:

- Enrolled devices – Total number of devices registered and assigned to your organization
- Managed rooms – Total number of rooms with at least one assigned device in your organization
- Team members – Total number of users with active accounts in your organization

To identify devices that require attention, a filtered device list is displayed, showing only devices that currently report issues. Devices are sorted based on their level of urgency.

> **i** Devices with no issues detected are not shown in the list. Therefore, the number of enrolled devices can differ from the number of devices in the device list on the Dashboard.

Possible device-level issues

Issues that can occur at the device level are divided into the following categories:

- Cloud alerts – Devices that are currently disconnected from the cloud and cannot be monitored or managed remotely.
- Device alerts – Critical alerts for connected devices that require immediate attention.
- Device warnings – Non-critical notifications for connected devices that may indicate misconfiguration.
- Firmware state – Firmware notifications for connected devices that may need attention.

State colors based on urgency

> **i** If a device reports a critical alert in addition to a warning or firmware notification, it is represented as red.

The state of the device is color-coded based on the urgency:

- Red – Disconnected devices or devices with critical alerts
- Yellow – Devices with warnings
- Blue (update available): new firmware is available to be installed
- Red (update failed) – Firmware update unsuccessful

Issue-based device list filtering

The device list on the Dashboard can be filtered by issue.

> **i** Only one filter can be applied at a time.

To filter the device list:

- ▶ Select the tile representing Cloud alerts, Device alerts, Warnings, or Firmware to filter the device list.
- ▶ Deselect the tile to remove the filter from the list.

Device states

The device information row in the device list, either on the Dashboard or on the Device overview page, represents the reported state of the device. The number of represented states is limited to one. An indicator provides insight into the number of reported issues.

For detailed information, go to the Device detail page to see all states that are reported for a specific device.

> **i** If a device reports a cloud alert, device alert, or warning, all users within the organization are notified by email containing the specific organization, device, issue, and the device's location.

Enabling or disabling daily device status reports

Enable a daily device status report to receive regular notifications about critical failures and warnings.

The latest status report provides current device conditions that require your attention, helping you stay informed and take action when necessary; the report is sent every morning (CET timezone) to your registered email address.

To enable or disable the daily status report on your devices:

- In DeviceHub, go to **Settings** at the bottom left of the navigation bar.
- In the field **Latest device status email**, set the toggle to **On** or **Off** to enable or disable the report.

✓ You have successfully enabled or disabled the daily device status report.

Updating device firmware

The currently installed firmware for each device is shown in the device list and on the Device detail page.

The availability of new firmware updates is indicated by 'Update available', which is also visible on the dashboard. On DeviceHub, you can always update to the latest available version. Downgrading or selecting a specific (earlier) version is not possible.

> **i** The firmware installation may take several minutes and includes a reboot of the device. Please do not interrupt the process. After updating, the device will automatically reconnect to DeviceHub.

To update the firmware for a device:

- Navigate to the Dashboard, the Device overview page, or the device detail page.
- Click on **Update available**.
- Review the release notes of the update and accept the license agreement by checking the box to proceed.
- Click on **Update**.
  - During the update process the firmware state changes to 'Updating'. After successful installation, the device will show the label 'up to date' and display the new firmware version.

    > **i** If the firmware update fails, it will be indicated by a label 'Update failed'. Click it to find out more about the issue and to restart the update process.

✓ The firmware of your device has been updated successfully.

Room assignment

Manage room assignments for devices by assigning, changing, or removing their room assignments through the device overview or detail pages.

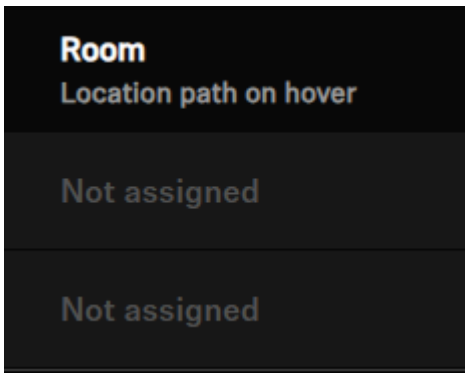
To organize your devices based on your location setup, devices can be assigned to a room. This can be either done on the Device overview page or on the specific device detail page.

> **i** Please note that assigning rooms can only be done by a user who is assigned to the **Owner** role.

Assigning device to a room

Audience: Owner

Manage room assignments for devices by assigning, changing, or removing them through the Device overview page, detail pages, or the location page.



> **i** Only connected devices without an existing room assignment can be selected.

To assign a device to a room via the Device overview page:

- Click on:
  - **Not assigned** in the room assignment section in the device list or
  - on the icon button next to the device and choose **Manage room assignment**.
- Select the room which you want to assign the device to.
- Click on **Save** to reflect the changes in the device list.

To assign a device to a room via the Device detail page:

- Click on the **device name** to enter its device detail page.
- Click on the status **Not assigned** in the core information section.

- Select the room which you want to assign the device to.
- Click on **Save** to reflect the changes in the device list.

To assign a device to a room via the location page:

- Click on the icon button next to the specific room and choose **Assign device**.
- Select the device which you want to assign to the room.
- Click on **Save** to reflect the changes in the device list.

✓ Your device has been assigned to a room.

Changing room assignment

Instructions for changing a device's room assignment via the Device overview page or Room page.

To change the room assignment of an already assigned device via the Device overview page:

- Click on the icon  next to the device and choose **Manage room assignment**.
- Choose the option **Change room assignment**.
- Select the room which you want to assign the device to.
- Click on **Save** to reflect the changes in the device list.

To change the room assignment of an already assigned device via the room page:

- Click on the **room name** to which the device is currently assigned to.
- Choose the option **Change room assignment**.
- Select the room which you want to assign the device to.
- Click on **Save** to reflect the changes in the device list.

✓ The room assignment for an existing device has been updated.

Removing room assignment

Audience: Owner

Instructions for removing a device's room assignment via the device overview page.

> **i** When deleting a room with devices assigned to it, the devices remain in the organization's device list. They can be reassigned to any other room later.

To remove the room assignment via the Device overview page or Room page:

- Click on the icon  next to the device and choose **Manage room assignment**.
- Choose the option **Remove room assignment**.
- Confirm to remove the room assignment and changes will be reflected in the device list.

> ✓ The room assignment for an existing device has been removed.

Account settings

Here you can manage your account settings, including custom appearance, password, and membership.

Manage your account by:

- Admin approval to enable trust between tenants
- Editing account information
- Changing your account password
- Editing organization information
- Changing display settings
- Leaving an organization
- Deleting organization
- Enabling or disabling daily device status reports

Admin approval to enable trust between tenants

Audience: It-admin

Administrators manage Microsoft permission consent requests and, once approved, users in the tenant can sign in to the Sennheiser screen with their Microsoft accounts.

As an admin, you are notified when there is a pending approval request. For more information about these requests, see the Microsoft documentation: Request permissions that require administrative consent.

As an admin, you can decide whether to grant or revoke permissions. After you grant the permissions, users in this tenant can use their Microsoft accounts to sign in on the Sennheiser screen.

Editing account information

Learn how to edit your account information.

To edit your personal Sennheiser account information:

- Navigate to the page **Settings**.
- In the section **Personal**, click **Edit**.
- Edit your personal data.
- Click **Save**.

Your account information has been updated.

Changing your account password

Learn how to change your account password.

> Changes to your personal account information apply to all connected Sennheiser products and platforms.

To change your password, request a new password on the login page:

- Go to devicehub.com.
- Click on **Forgot your password?**.
- Follow the on-screen instructions to set a new password.

Your account password has been updated.

Editing organization information

Audience: Owner

Edit your organization's information.

> **i** Organization settings apply across the organizational workspace to all team members. Only a user assigned the **owner** role can manage the organization's data.

To edit your organization settings:

- On the page **Settings**, navigate to the section **Organization** and click **Edit**.
- Edit your organization's data.
- Click **Save**.

✓ Your organization's information has been updated.

Changing display settings

Change your display settings.

> Display settings apply only to your user account and to all organizations you belong to.

To change your display settings:

- Navigate to the **Settings** page.
- In the **Display** section, adjust the display settings to your preference.
- When you choose a setting, it is saved.

Your display settings have been updated.

Leaving an organization

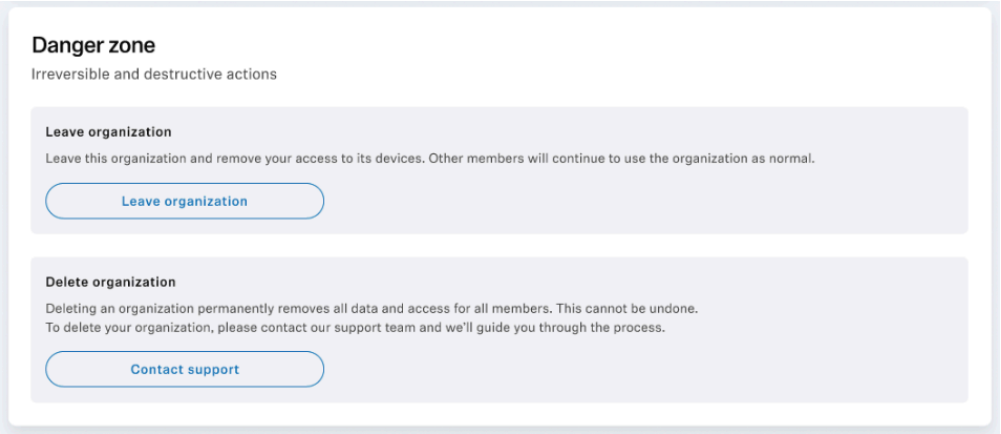
Instructions for leaving an organization.

After you leave an organization, you will be redirected either to the Login page or to another organization you belong to. The organization you left will no longer appear in the organization dropdown in the navigation bar.

> **i** There must be at least one owner in each organization. Before you can leave, invite other team members or promote someone to the owner role. If the organization is no longer needed, request its deletion from our support team.

To leave the organization:

- Navigate to the **Settings** page.
- In the **Danger** zone, select **Leave organization**.



- Confirm that you want to leave in the confirmation modal and then close the modal.

✓ You have successfully left the organization.

Deleting organization

Audience: Owner

Instructions for deleting the organization.

> **i** Before deleting the organization, you must remove all team members. Only users with the owner role can delete an organization.

To delete the organization:

- Navigate to the **Settings** page.
- In the **Danger** zone, click on **Contact support**.
- Fill out the form with your request and submit it to the Sennheiser support team.
  - The Sennheiser support team will contact you by email to confirm the deletion.

> ✓ You have successfully initiated the organization's deletion process. The Sennheiser support team will contact you regarding the deletion status.

Sennheiser electronic SE & Co. KG | Am Labor 1 | 30900 Wedemark | Germany