



DeepHub Meeting

User's Manual



Foreword

This manual introduces the instructions for using the DeepHub Meeting software. Please read it carefully before using the software. After reading, please save the document properly for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable result.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Content

Foreword	II
1 Activation	1
1.1 Activation	1
2 Function Description	2
2.1 Home Screen	2
2.2 Attend a Meeting	2
2.2.1 Attending a Meeting by Entering the Meeting ID	2
2.2.2 Roles in a Meeting	3
2.2.3 Recent Contacts	4
2.3 Instant Meeting	5
2.4 Meeting Reservation	5
2.5 Basic Operations in a Meeting	6
2.5.1 Raising Hand (Apply to Speak)	6
2.5.2 Microphone/Camera/Speaker	6
2.5.3 Comments	7
2.5.4 Hide Menu	7
2.5.5 Invitation	7
2.5.6 More	7
2.5.7 Layout	8
2.5.8 Meeting Settings	8
2.5.9 Exit a Meeting	9
2.6 Host Management	10
2.6.1 Participant List	10
2.6.2 Changing Roles	10
2.6.3 Controlling Microphone and Camera	12
2.6.4 Changing Names of Participants	13
2.6.5 Removing Participants from Meeting Room	13
2.7 Sharing Screen	14
2.7.1 Starting Sharing	14
2.7.2 Stopping Sharing	14
2.8 Interactive Whiteboard	14
2.8.1 Using Interactive Whiteboard	14
2.8.2 Exiting Interactive Whiteboard	15
2.9 Recording	16
2.9.1 Starting Recording	16
2.9.2 Stopping Recording	16
2.10 Settings	16
2.11 Schedule	18
2.11.1 Basic Schedule	18
2.11.2 History	19
2.11.3 Meeting Details	19

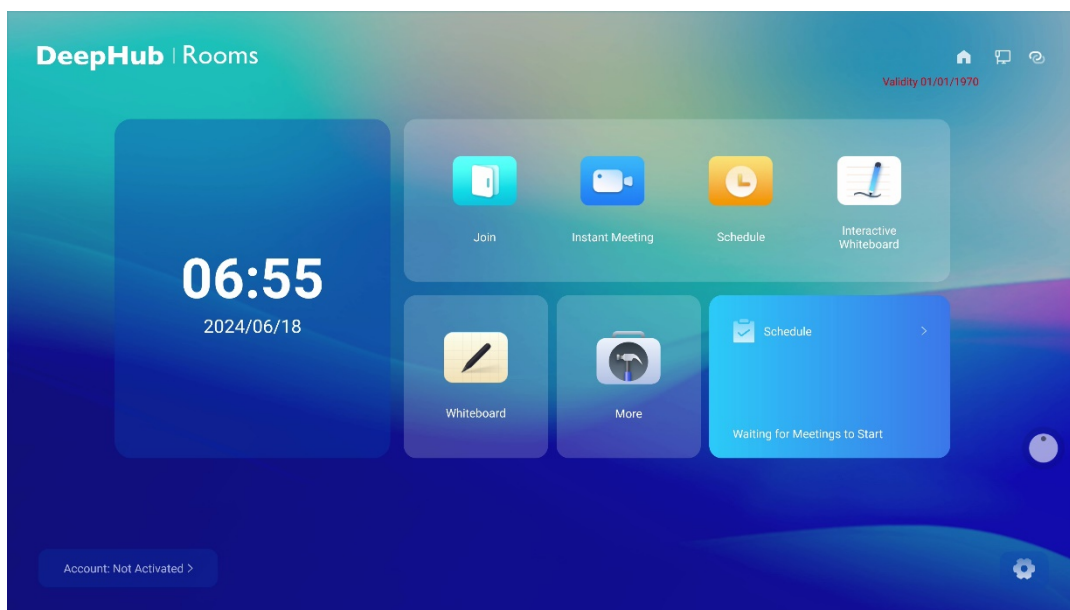
2.11.4 Traffic Restriction for Video Storage and Viewing	20
2.12 Whiteboard	20
2.13 More	21
3 FAQ	22
Appendix 1 Security Commitment and Recommendation	23

1 Activation

1.1 Activation

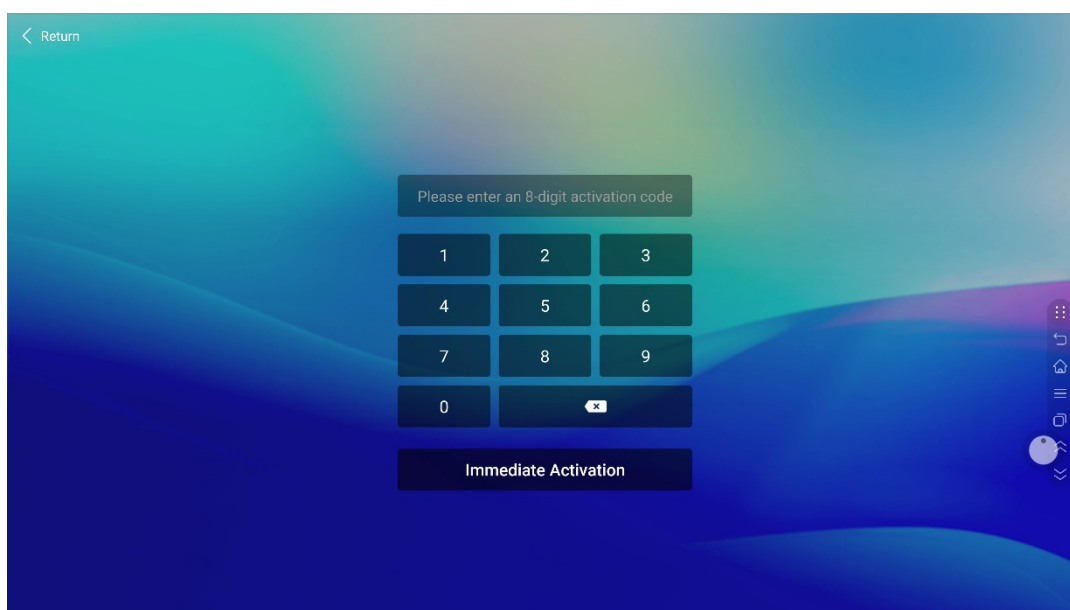
When you open the software, if it is not activated, you will see **Account: Not Activated** in the bottom left corner of the home screen.

Figure 1-1 Account not activated



Tap **Account: Not Activated** to enter your activation code. If correct you can activate the meeting function.

Figure 1-2 Activation

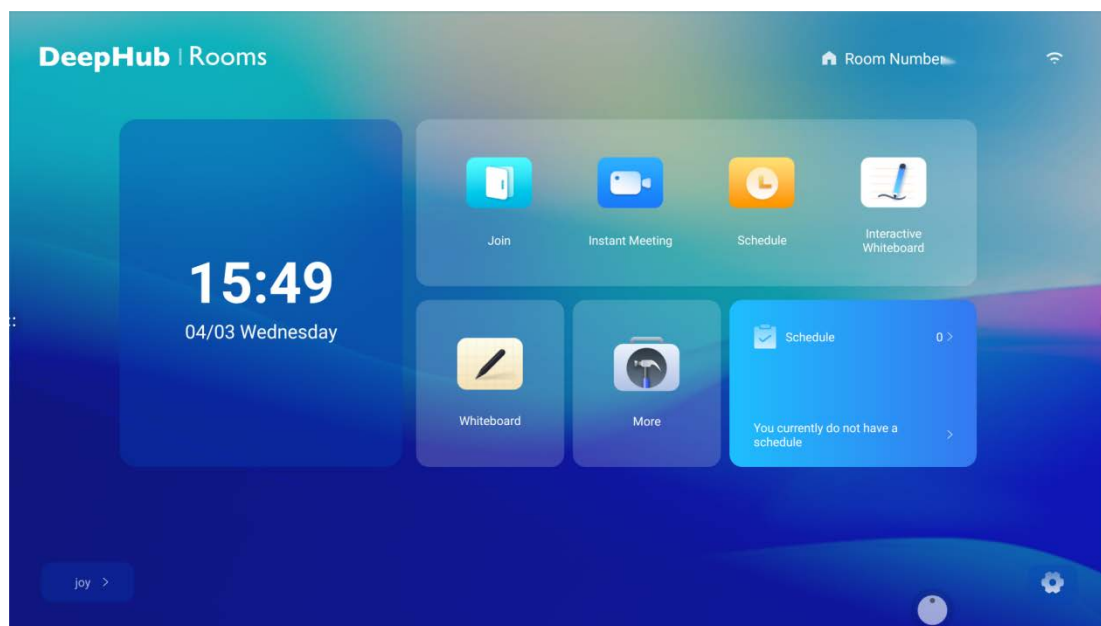


After activation, you can edit the account name by yourself.

2 Function Description

2.1 Home Screen

Figure 2-1 Home screen



The homepage screen is the main screen for you to interact with the DeepHub Meeting system, providing the following quick access and functional modules:

- **Time:** Display the current system date and time.
- **Join:** Quickly join an existing meeting by entering the meeting number.
- **Instant Meeting:** Create a new meeting immediately and invite others to join.
- **Schedule:** Set the meeting time, topic, and other information in advance to schedule a meeting.
- **Interactive Whiteboard:** A whiteboard for real-time collaboration and annotation.
- **Whiteboard:** A whiteboard for writing and annotation in on-premises environments.
- **More:** Includes advanced features such as system settings and viewing schedules.
- **Schedule:** View and manage your meeting schedule.
- **Settings:** Adjust system parameters and configurations.
- **Account:** Manage your account information and device name.

2.2 Attend a Meeting

2.2.1 Attending a Meeting by Entering the Meeting ID

Step 1 Tap **Join**.

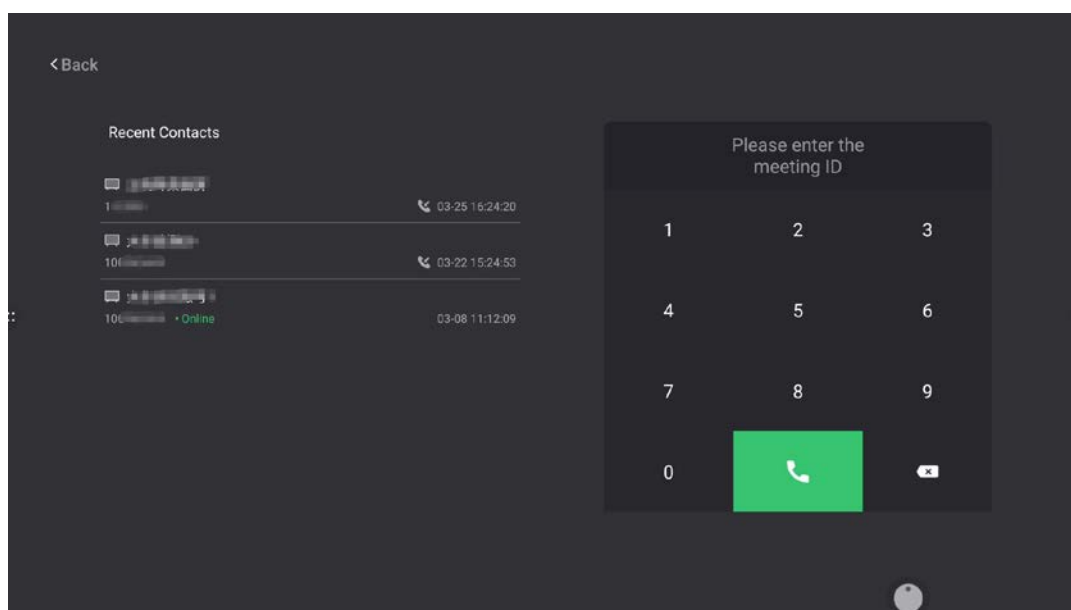
Step 2 Enter the meeting ID in the pop-up input box.

Step 3 Tap the call button, and then the system will try to connect to the meeting.



According to the actual situation of the meeting, if the meeting is completely open, you can directly enter the meeting. If the meeting is private, you cannot join it.

Figure 2-2 Joining a meeting



2.2.2 Roles in a Meeting

The main roles in the meeting are host, guest and audience.

2.2.2.1 Host

- **Host:** The host has the highest permissions over the meeting, including to invite and remove participants, manage microphone and camera, and record the meeting.
- **Guest:** The guest can speak, share screen and use whiteboard, but does not have all permissions of a host.
- **Audience:** The audience can only view meeting content, and unable to engage in audio and video interaction.

Figure 2-3 Host operation bar



Functions for the host:

- **Active Settings:** Actively configure the microphone and camera. Guests can turn on/off by themselves.
- **Share:** Share screen and interactive whiteboard.
- **Basic Operations:** Adjust speaker volume, set the window layout, the resolution of camera, and screen sharing.
- **Record:** Tap to start recording.
- **Security:** The host can tap the security icon to enter the security settings screen during the meeting.

- **Host:** Tap to view meeting information and manage the meeting permissions.

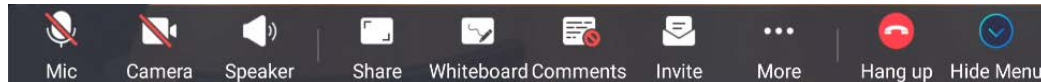


Guests of tourists cannot be set as hosts (tourists are not allowed to be set as hosts)

2.2.2.2 Guest

Guests can enable microphone and camera, speaker, screen sharing, interactive whiteboard, comments, invitations and more.

Figure 2-4 Guest Operation Button



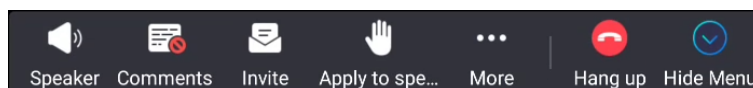
Functions for the guest:

- **Active Settings:** Actively configure the microphone and camera. Guests can turn on/off by themselves.
- **Share:** Share screen and interactive whiteboard.
- **Basic Operations:** Adjust speaker volume, set the window layout, the resolution of camera, and screen sharing.

2.2.2.3 Audience

The audience can enable speaker, comments, invitation, request to speak and more.

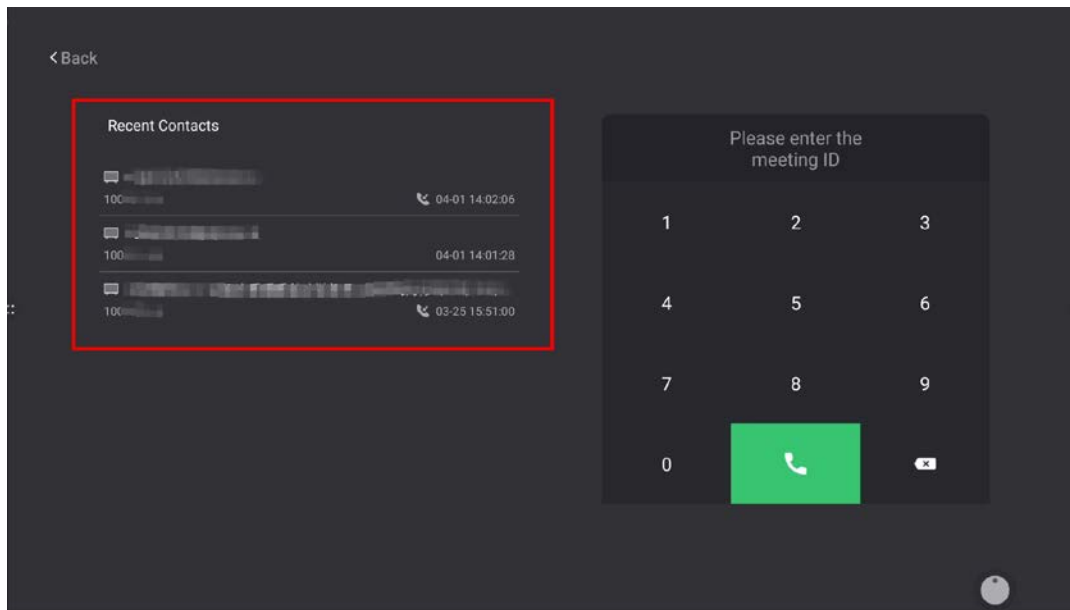
Figure 2-5 Audience Operation Button



2.2.3 Recent Contacts

The recent contacts display the users who have recently joined the meeting and the users who have recently called. User's name, meeting ID, and time are also displayed.

Figure 2-6 Recent Contact



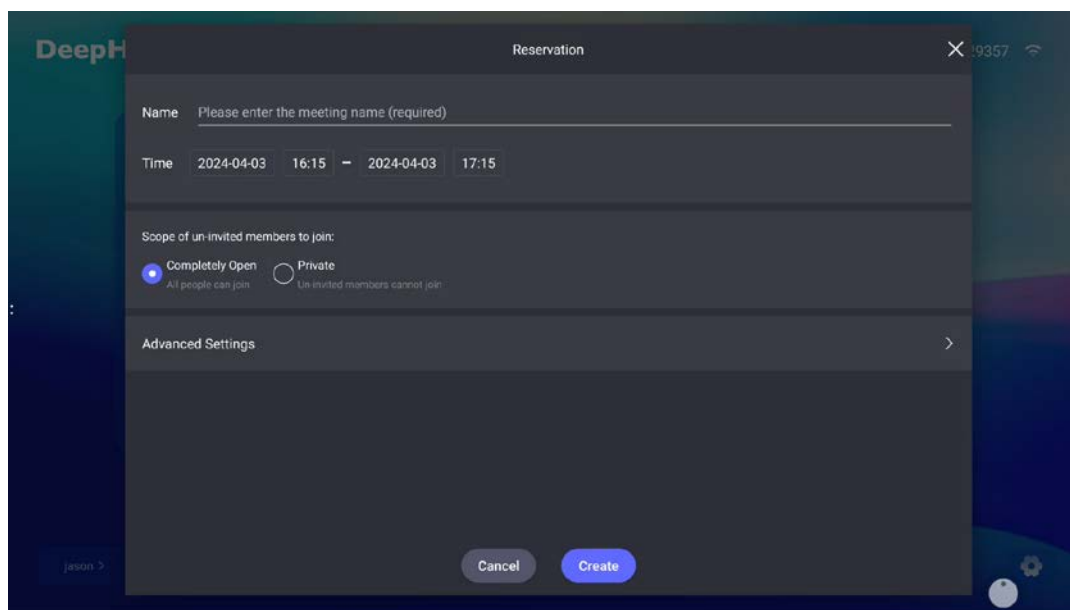
2.3 Instant Meeting

Instant meeting allows you to quickly create and join a new meeting. Just tap **Instant Meeting**, and then the system will automatically create and enter the meeting screen.

2.4 Meeting Reservation

- Step 1 Tap **Reservation**.
- Step 2 Enter the meeting name, time and participant information in the reservation screen.
- Step 3 Select whether the host's approval is required for participants to join the meeting.
- Step 4 (Optional) Set the meeting password to secure the meeting.
- Step 5 Tap **Create**, and then your reservation will be saved and displayed on the **Schedule** screen.

Figure 2-7 Meeting reservation



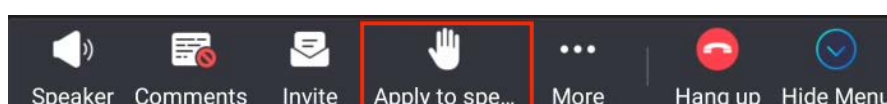
2.5 Basic Operations in a Meeting

Basic operations in a meeting include configuring camera, microphone, and speaker, viewing participant information, managing layout and meeting.

2.5.1 Raising Hand (Apply to Speak)

As an audience member, when you want to speak in the meeting, you can tap **Apply to Speak**. The host will receive your request and decide whether to grant you the speak permission.

Figure 2-8 Apply to speak



2.5.2 Microphone/Camera/Speaker

- **Turn on/off microphone:** Tap **Mic** to control your microphone to speak or mute in the meeting.
- **Turn on/off camera:** Tap **Camera** to enable or disable the camera.
- **Adjust the speaker volume:** Tap **Speaker** to mute or adjust the volume.

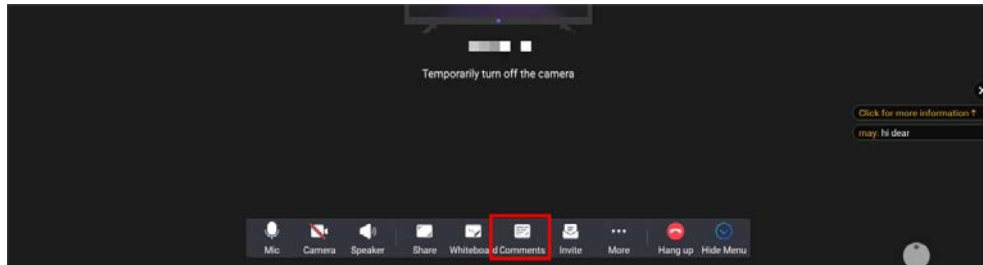
Figure 2-9 Microphone/camera/speaker



2.5.3 Comments

In a meeting, you can tap **Comments** to communicate with other participants by text.

Figure 2-10 Comments



2.5.4 Hide Menu

Tap **Hide Menu** to hide the function bar. You can also tap to display the function bar again.

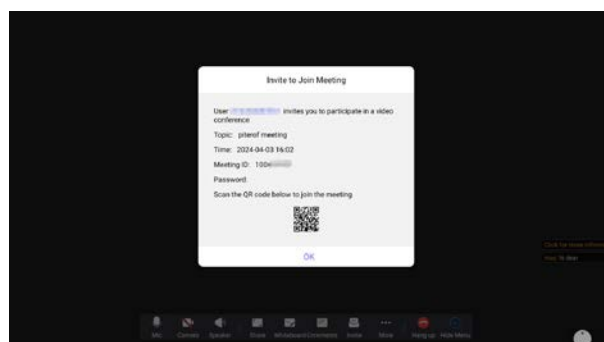
Figure 2-11 Fold Up



2.5.5 Invitation

Tap **Invite**, and then copy and send the meeting ID or the joining link to others to invite them to join the meeting.

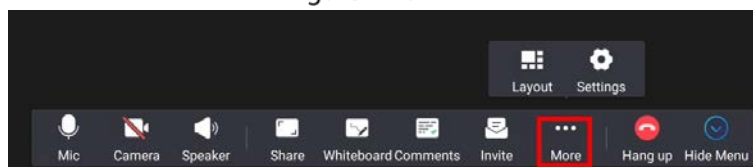
Figure 2-12 Invitation



2.5.6 More

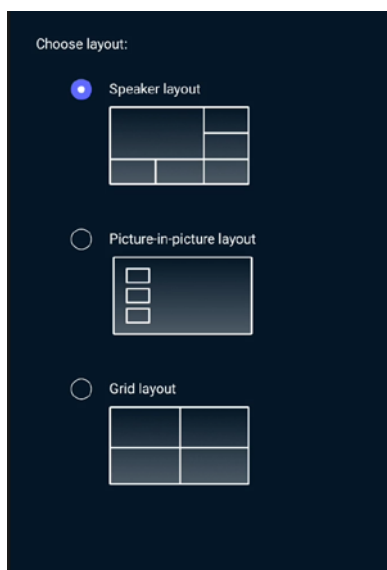
Tap **More** to configure more meeting settings, such as adjusting the layout, enabling pure audio mode and lab functions.

Figure 2-13 More



2.5.7 Layout

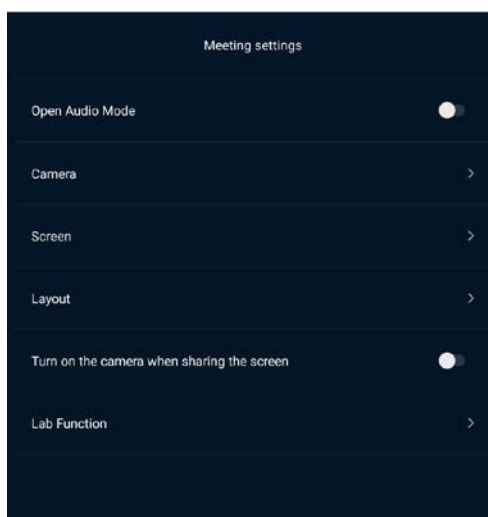
All meeting members can set the layout, including speaker, picture-in picture, and grid layouts. It is speaker layout by default.



2.5.8 Meeting Settings

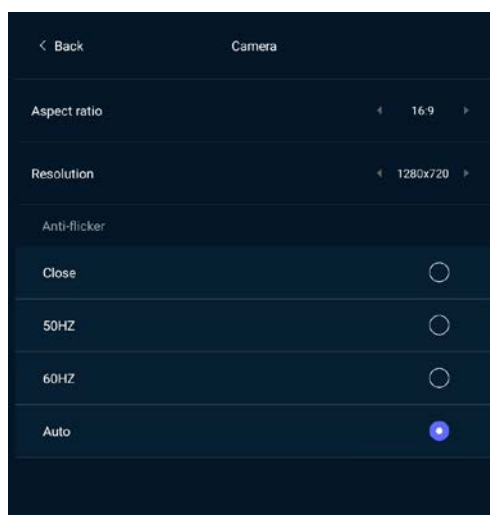
The parameters of meeting settings might vary depending on the meeting member roles. The common configuration supports configuring audio mode, layout, and lab function. Only hosts and guests can configure the camera and screen resolution, and the camera can be turned on or off during screen sharing.

Figure 2-14 Meeting settings



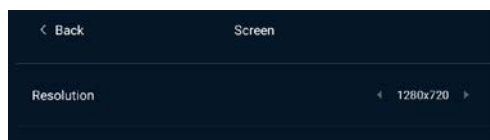
- Camera:** Configure the aspect ratio, resolution (360p, 480p, 720p, and 1080p), and anti-flicker of this device camera:

Figure 2-15 Camera settings



- **Screen:** Configure the resolution of the screen (720p, and 1080p)

Figure 2-16 Screen sharing settings



- During screen sharing, you can enable the camera. It is disabled by default. When screen sharing is enabled, there are two images, namely video and screen sharing images.

2.5.9 Exit a Meeting

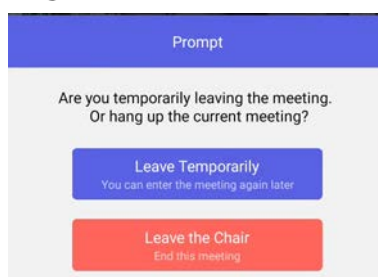
Tap **Hang Up** at the bottom right of the screen to exit the current meeting. The host can choose whether to leave temporarily or end the whole meeting.



When the host hangs up, please carefully choose whether to leave or end the meeting.

- **Leave Temporarily:** The host leaves the meeting, and others can continue the meeting in the current meeting room.
- **Leave the Chair:** The meeting is ended, and everyone in the meeting is kicked out of the meeting room.

Figure 2-17 Exiting a meeting



2.6 Host Management

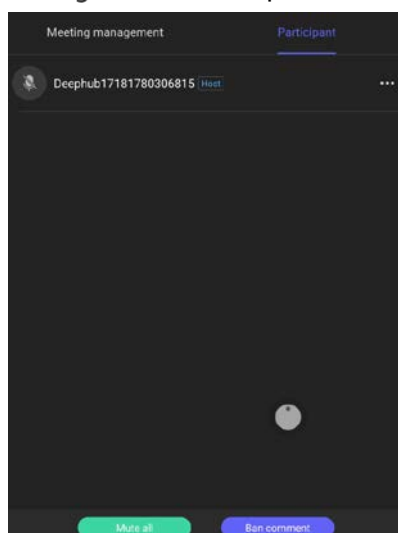
The host can view and manage the participant list, including viewing the participant status, identity, name, and more. The host can also mute all the participants.

2.6.1 Participant List

List in the meeting: one of the hosted management pages, including the list of participants

- **Participant List:** Displays the microphone status, attendee name, and role.
- **Role:** Host, guest, and audience.
- **Meeting Management:** The host can tap ... to separately configure settings for participants.
- **Mute all:** tap **Mute all**, and then all participants cannot speak in the meeting room.
- **Ban comment:** Tap **ban comment**, and then all participants cannot comment in the meeting room.

Figure 2-18 Participant list

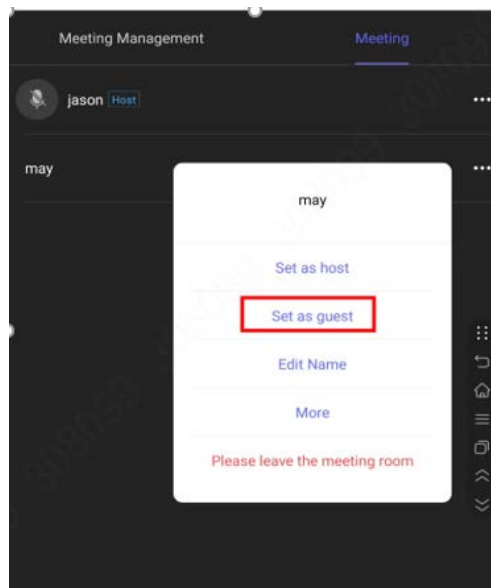


2.6.2 Changing Roles

A host can change the role of a participant, such as changing audience members to guests to allow them to speak.

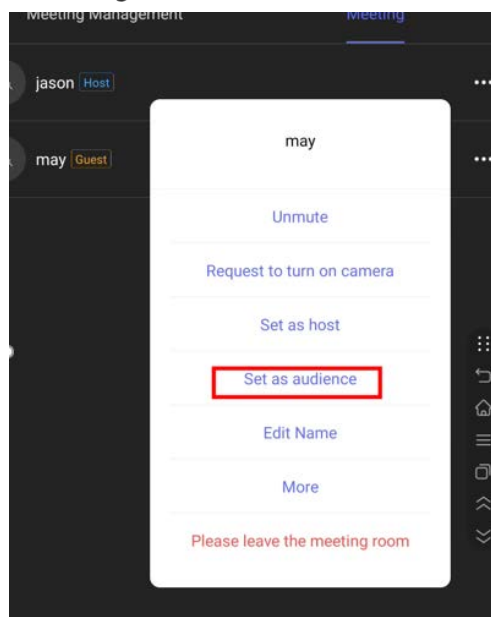
- **Set as guest:** Participants with audience identity and host identity can be set as guests. Microphone, speaker, screen share, interactive whiteboard and other functions cannot be performed after being set as a guest.

Figure 2-19 Set as guest



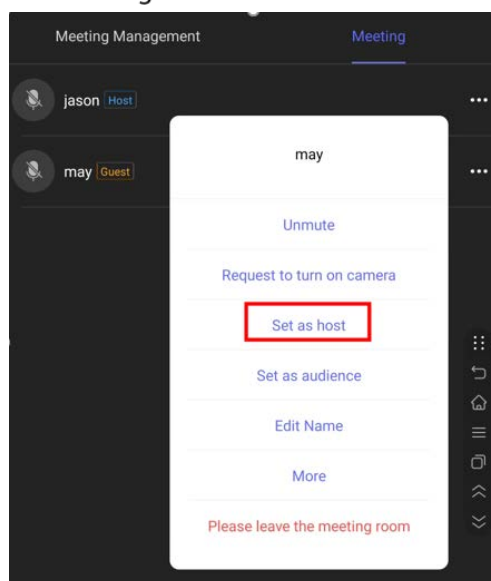
- Set as audience:** Participants with guest identity and host identity can be set as audience. After being set as an audience, you can only attend the meeting but cannot perform other functions.

Figure 2-20 Set as audience



- Set as host:** Participants with guest identity and audience identity can be set as hosts. After being set as a host, it has all the functions of a guest, and also has the permission of hosting and meeting management. Tourist cannot be set as host.

Figure 2-21 Sett as host

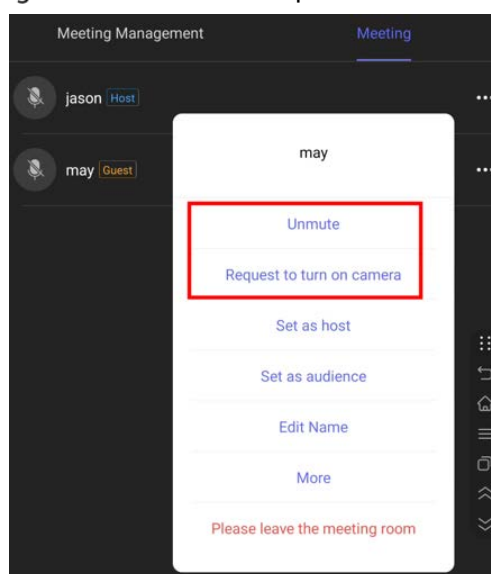


2.6.3 Controlling Microphone and Camera

The host can enable and disable microphone and camera of the participants to ensure the order of the meeting.

- Request to turn on microphone/camera: The host can select guests to apply for turning on microphone and camera respectively
- Application received: The participant receives the application to turn on the microphone and camera notification on the pop-up window.
- Application processing: The participant can choose **Reject** or **Allow**. If the application is not processed for more than 60 s, the host can apply for again after timeout.

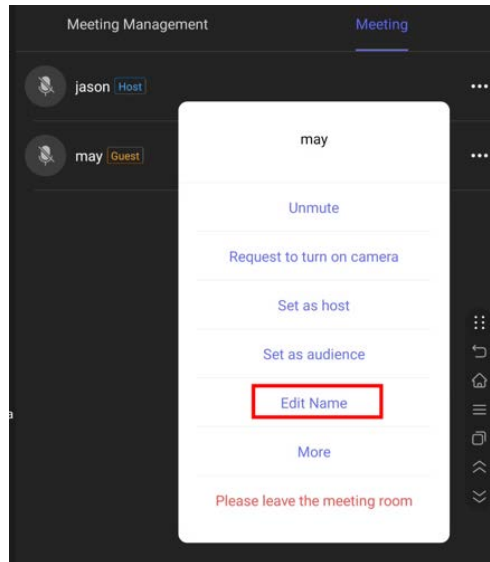
Figure 2-22 Control microphone and camera



2.6.4 Changing Names of Participants

The host can directly modify the name of participants in the participant list.

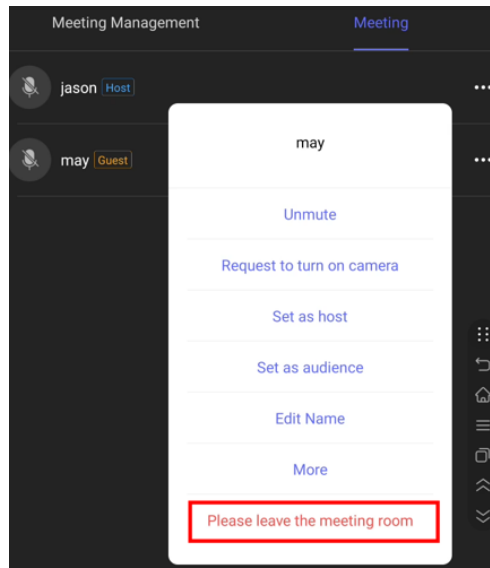
Figure 2-23 Renaming



2.6.5 Removing Participants from Meeting Room

The host can remove participants who do not need to be in the meeting. Once removed, the participants exit from the meeting.

Figure 2-24 Remove participants

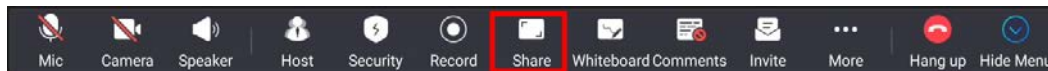


2.7 Sharing Screen

2.7.1 Starting Sharing

In a meeting, tap **Share** and confirm to begin sharing your screen, and then other participants can view your screen.

Figure 2-25 Sharing



- When you want to view a more high-definition image during screen sharing, tap the **More > Settings > Screen** in the meeting to set the resolution of the screen to 1080p. You can also view and change the resolution on the meeting settings screen,
- Whether the shared resolution supports 1080p depends on the attributes of the meeting room account.

2.7.2 Stopping Sharing

To stop screen sharing, tap the **End Sharing** that hovers on the screen.

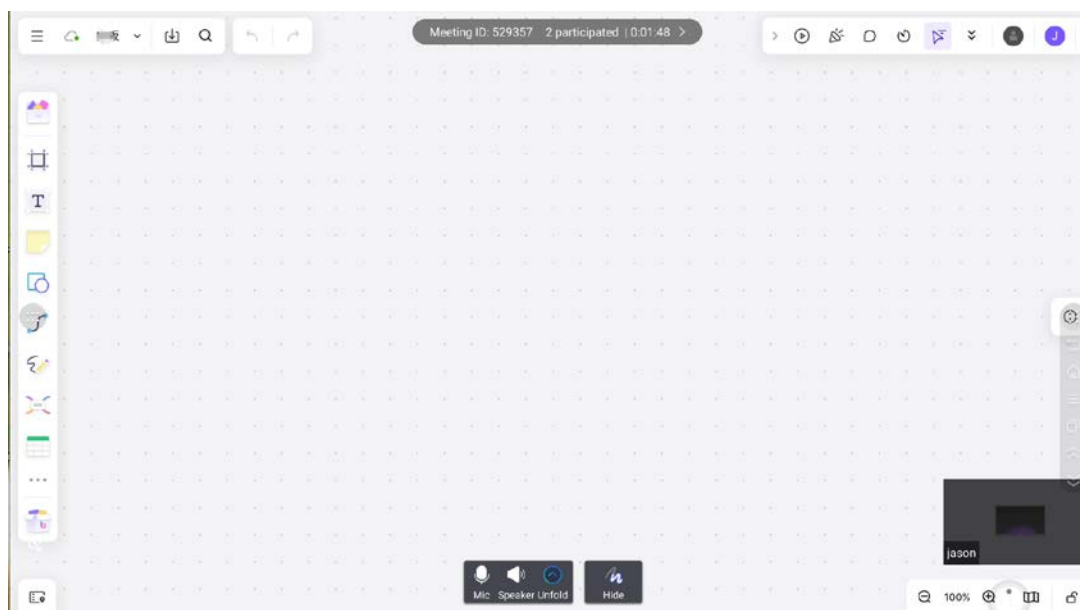
2.8 Interactive Whiteboard

2.8.1 Using Interactive Whiteboard

According to whether the account configuration has the permission of interactive whiteboard, only the activation code contains interactive whiteboard permission can initiate the interaction. After initiating the interactive whiteboard, you can quickly create a meeting and enter the whiteboard page for interactive drawing.

The logic of the video window in the interactive whiteboard: The video window in the lower right corner of the interactive whiteboard changes with the voice activation, prioritizing the display of the image of the speaker.

Figure 2-26 Interactive whiteboard



When initiating a whiteboard session or not exiting the interactive whiteboard, other participants can select to hide or display the whiteboard.

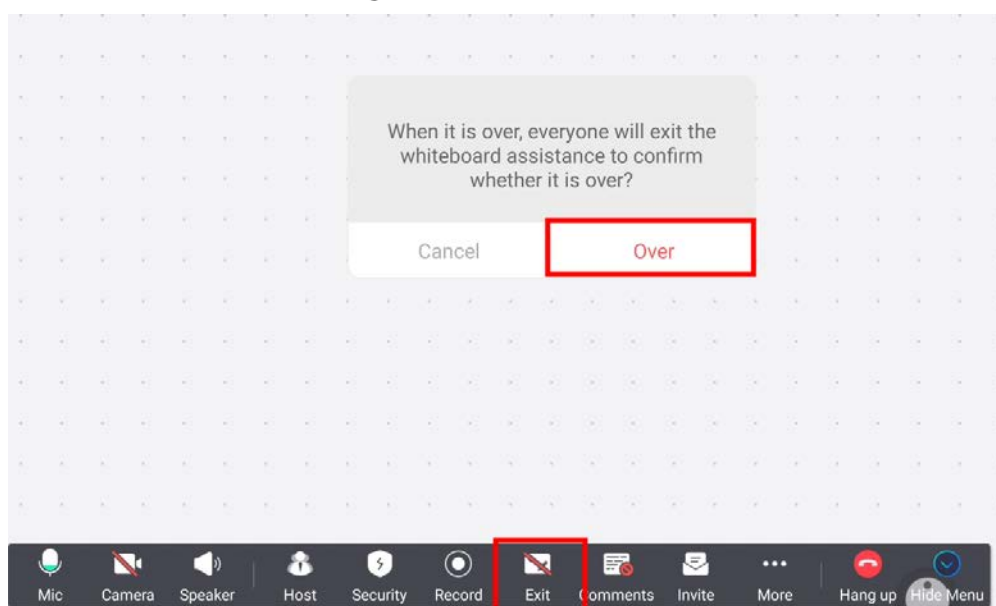
Figure 2-27 Hide Interaction



2.8.2 Exiting Interactive Whiteboard

Only the host can exit the interactive whiteboard. After the host exits, all participants in the meeting exit the interactive whiteboard.

Figure 2-28 Exit whiteboard



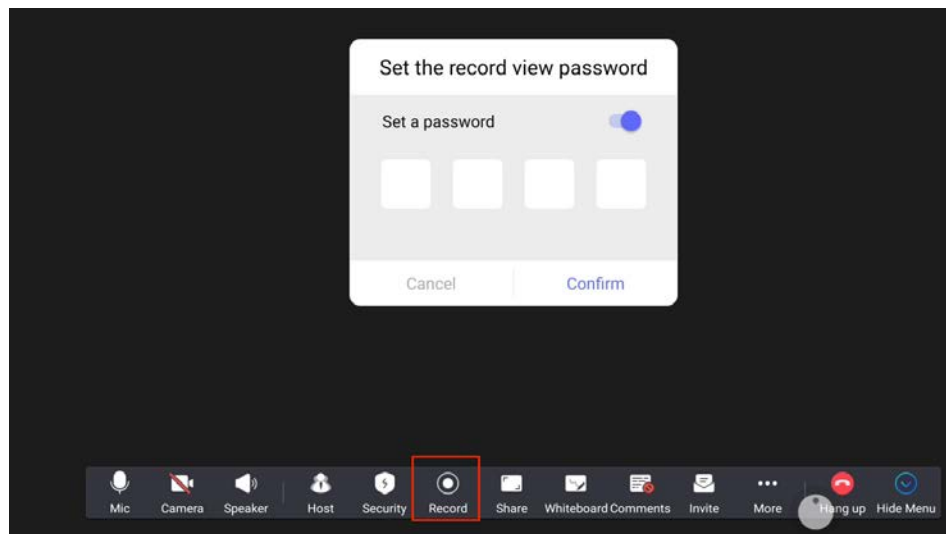
2.9 Recording

2.9.1 Starting Recording

Tap **Record** in the meeting, and then a pop up a window is displayed to ask whether to set the recording viewing password. If you set the password, you need to verify it every time you view the recording after the meeting.

After the recording is started successfully, the recording status and duration are displayed.

Figure 2-29 Recording



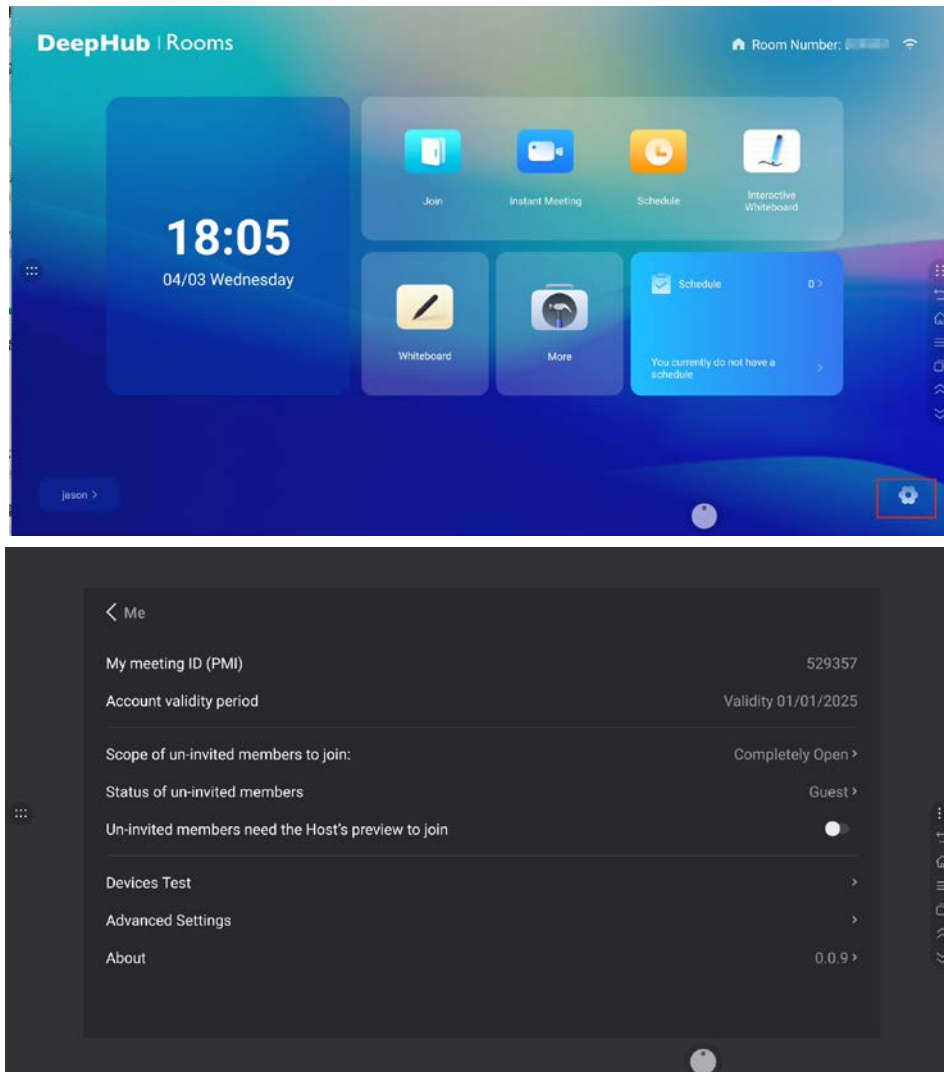
2.9.2 Stopping Recording

You can view the recording in History after the meeting is ended. The host can end the recording by tapping the **Record**.

2.10 Settings

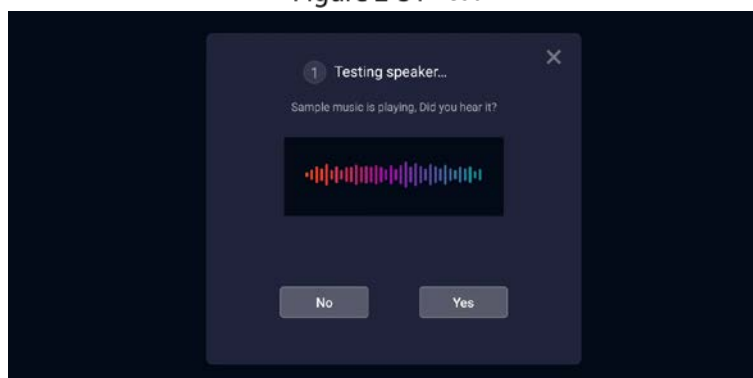
On the **Settings** screen, you can manage account information, configure meeting settings, debugging, and more. You can adjust settings for microphone, camera, network, and audio policies for your meeting.

Figure 2-30 Settings



- **Device Test:** Mainly tests the microphone, camera and speaker.

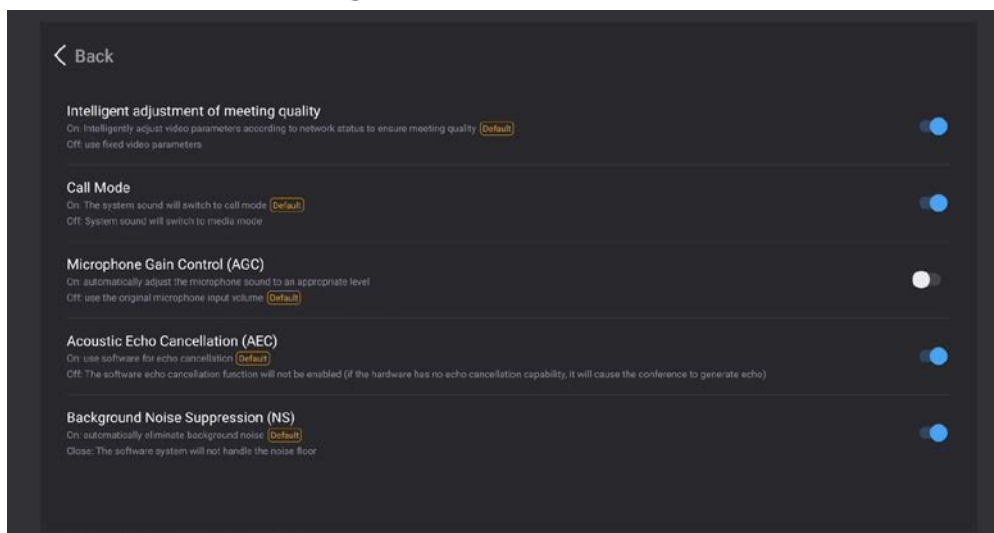
Figure 2-31 Test



- **Advanced Settings:** Mainly include dynamic strategy of weak network, call mode, AGC, AEC and NS settings.
 - ◇ **Intelligent adjustment of meeting quality:** Enabled by default. In case of poor network conditions, priority is given to ensuring sound quality, and the video will be adjusted according to the network conditions, including switching between different video streams. In extremely poor conditions, the video might not be subscribed.
 - ◇ **Call Mode:** Default system call mode.

- ◇ **Microphone Gain Control (AGC):** Enabled by default. It automatically adjusts the microphone volume to an appropriate level.
- ◇ **Acoustic Echo Cancellation (AEC):** Enabled by default. It effectively eliminates echo during communication.
- ◇ **Background Noise Suppression (NS):** Enabled by default. The software automatically filters and eliminates background noise.

Figure 2-32 Advanced Settings



2.11 Schedule

On the **Schedule** screen, you can view and manage your meeting schedule. You can edit the information of a meeting that has not started, or view the meeting details in the history.

2.11.1 Basic Schedule

All scheduled meetings will be displayed in the calendar. The calendar displays the current date by default. The number of scheduled meetings for each date is displayed on top of the date. On the left side, there is information corresponding to the calendar. Taping **Details** to view the details of the scheduled meetings.

Figure 2-33 Schedule



- Tap **History** in the lower left corner of the **Schedule** screen to view the history list.
- Recorded videos can be viewed and deleted in the history. To ensure the security of videos, you need to enter the corresponding PIN code to view videos.

Figure 2-34 History



The detailed information of the meeting report includes meeting name, meeting number, time, initiator, number of participants, meeting duration, participation details and duration.

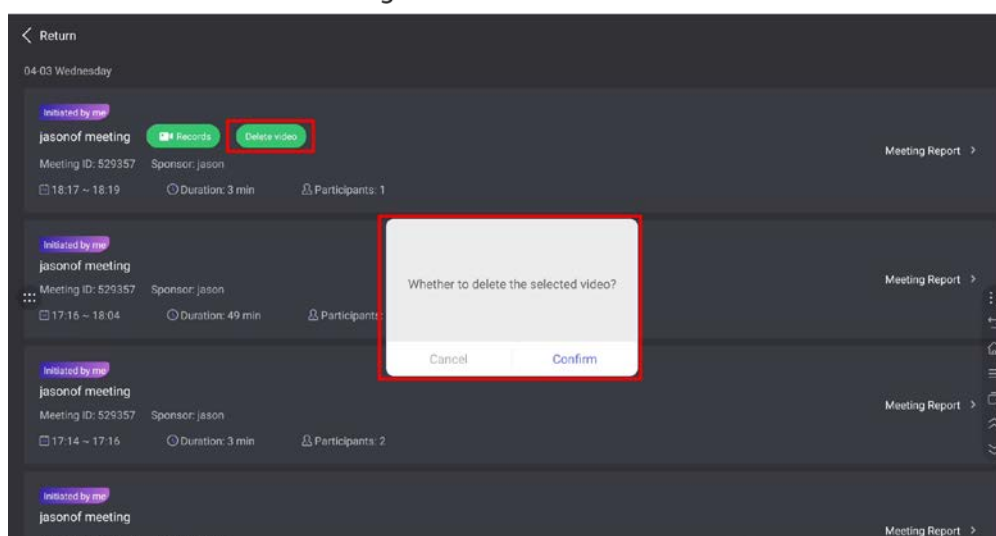
Figure 2-35 Meeting details



2.11.4 Traffic Restriction for Video Storage and Viewing

Each device account has restriction on cloud storage space and download traffic restriction. When you tap **Record** but the storage is full, you are prompted to delete the existing video to release storage space as shown in the figure:

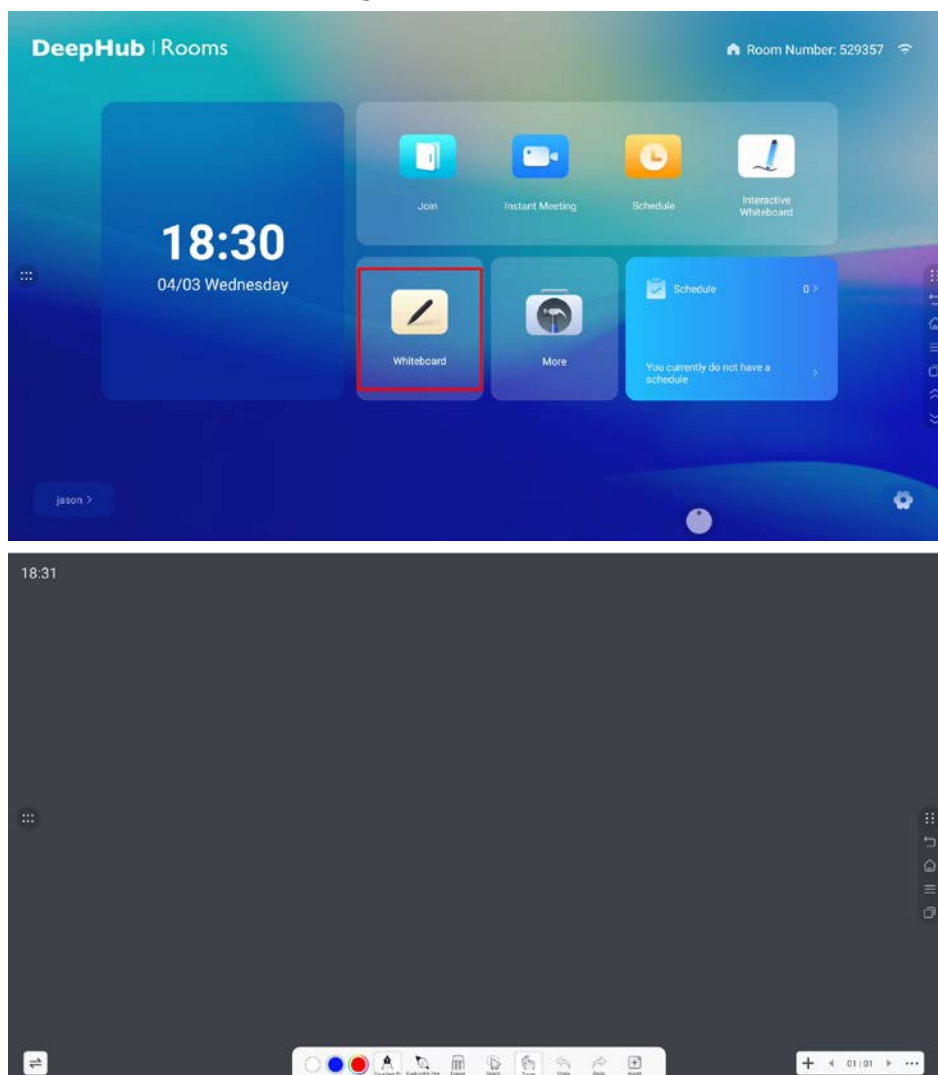
Figure 2-36 Delete videos



2.12 Whiteboard

This function enables you to write and annotate on local. This feature does not involve interaction with other members.

Figure 2-37 Whiteboard



2.13 More

Tap **More** to access all locally installed apps, such as file manager and browser.

3 FAQ

1. What should I do if there is a howling in the meeting?

- Howling is generated when more than one device is connected to the meeting in the venue.
- Solution: Turn off the microphone and speaker of all devices in the venue simultaneously and then only turn on the microphone and speaker of one device.

2. What if there is an echo in the meeting?

- Echo is caused by the sound from the device speaker being picked up by the microphone and then being transmitted back into the meeting. If other participants can hear the echo but you cannot, it is likely that the echo is coming from your device.
- Solution:
 - ◇ Check the CPU and memory usage of your system. If the CPU or memory usage is too high, shut down unnecessary applications.
 - ◇ Keep the speaker and microphone as far apart as possible.
 - ◇ Reduce the volume of the speaker, it is recommended not to exceed 70% of the maximum volume.

3. What should be done if there is a buzzing noise when using a **directional microphone** during a meeting?

- The occurrence of noise in a meeting can generally be divided into the following two scenarios: first is all or most participants can hear the noise, second is other participants cannot hear the noise, only specific individuals can.
- Solution:
 - ◇ First scene: Check which participants are generating the noise, mute their microphone, and remind them to check their own audios.
 - ◇ Second scene: Check if any other player or voice chat software is running in the background of this device, and shut down them.

4. What should be done when the voice volume in the meeting fluctuates.?

- Possible causes:
 - ◇ The speaker's surrounding environment and the equipment itself have uncertain background noise, which leads to the failure of the sound noise reduction mechanism;
 - ◇ The uncertain high-energy sound transmitted by other participants suppresses the speaker's voice.
- Solution:
 - ◇ Try to be in a quiet meeting environment.
 - ◇ Use a headset or shotgun microphone

5. Why do I see a black screen?

Possible causes:

- The participant has no camera, or the camera works abnormally caused by hardware error, poor contact, and more.
- The cameras of participants are occupied by other apps.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua's official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

1. Account Management

1.1 Use complex passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters: upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use repeating characters, such as 111, aaa, etc.

1.2 Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

1.3 Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

1.4 Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

1.5 Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

2. Service Configuration

2.1 Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2.2 Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

2.3 Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

2.4 Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

3. Network Configuration

3.1 Enable Allow list

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

3.2 MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3.3 Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;

According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;

Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

It is recommended to check online users regularly to identify illegal users.

4.2 Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

4.3 Configure network log

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

5. Software Security

5.1 Update firmware in time

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

5.2 Update client software in time

We recommend you to download and use the latest client software.

6. Physical protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188