

**TE20 Videoconferencing Endpoint
V500R003C00**

Administrator Guide

Issue 01
Date 2016-09-01

Copyright © Huawei Technologies Co., Ltd. 2016. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://e.huawei.com>

About This Document

Overview

Before you use the product, refer to the product vendor for version mapping information and to confirm compatibility with other videoconferencing equipment.

This guide describes how to use the TE20 videoconferencing endpoint (TE20 or endpoint for short) in terms of conference experience, device control, address book management, maintenance, and fault diagnosis.






Intended Audience

This document is intended for but not limited to endpoint administrators.

An endpoint administrator has access to all functions on the endpoint web interface, and remote controlled user interface (UI).

Symbol Conventions

The symbols that may be found in this document are defined as follows.

| Symbol | Description |
|--|---|
|  WARNING | Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. |
|  DANGER | Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. |
|  CAUTION | Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. |
|  NOTICE | Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury. |
|  NOTE | Calls attention to important information, best practices and |

| Symbol | Description |
|--------|---|
| | tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration. |

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 01 (2016-08-10)

This issue is the first official release.

Contents

| | |
|--|-----------|
| About This Document | ii |
| 1 Administrator Guidelines | 1 |
| 1.1 Application Scope | 1 |
| 1.2 Requirements on an Administrator | 1 |
| 1.2.1 Basic Knowledge | 1 |
| 1.2.2 Environment and System Information | 1 |
| 1.2.3 Reference Documents | 2 |
| 1.3 How to Obtain Help | 3 |
| 2 Getting Started | 5 |
| 2.1 Understanding the Remote Control | 5 |
| 2.1.1 Background..... | 5 |
| 2.1.2 Remote Control Buttons | 5 |
| 2.1.3 Remote Control UI | 6 |
| 2.1.4 Unpairing a Remote Control..... | 7 |
| 2.1.5 Using the Simulated Remote Control | 7 |
| 2.1.6 Using a Keyboard or Mouse | 8 |
| 2.2 Understanding the Web Interface..... | 10 |
| 2.2.1 Background..... | 10 |
| 2.2.2 Configuring the Browser | 10 |
| 2.2.3 Logging In to the Web Interface | 11 |
| 3 Conference Operations Using the Remote Control | 13 |
| 3.1 Initiating a Point-to-Point Conference | 13 |
| 3.2 Joining a Conference | 15 |
| 3.2.1 Joining a Conference by Entering the Conference Access Code | 15 |
| 3.2.2 Joining an HD Video Conference over an IMS Network..... | 16 |
| 3.2.3 Joining a Conference Initiated by a Third-Party Videoconferencing Platform | 17 |
| 3.3 Conference Control..... | 18 |
| 3.3.1 Request Chair..... | 20 |
| 3.3.2 Release Chair | 21 |
| 3.3.3 Extend Conference..... | 21 |
| 3.3.4 Add Site | 22 |
| 3.3.5 Call Site | 23 |

| | |
|--|-----------|
| 3.3.6 Mute/Unmute MIC | 24 |
| 3.3.7 View Site..... | 25 |
| 3.3.8 Broadcast Site | 26 |
| 3.3.9 Disconnect Site | 26 |
| 3.4 End Conference | 26 |
| 3.5 Enabling the Do Not Disturb Function | 27 |
| 3.6 Starting Presentation | 28 |
| 3.7 Configuring the Conference Screen Layout..... | 29 |
| 3.8 Adjusting the Volume at Your Site | 30 |
| 3.9 Muting or Unmuting the Local Microphone..... | 31 |
| 4 Conference Operations Using the Web Interface | 32 |
| 4.1 Initiating a Point-to-Point Conference | 32 |
| 4.1.1 Initiating a Conference from the Call Page..... | 32 |
| 4.1.2 Initiating a Conference from the Address Book Page..... | 34 |
| 4.2 Joining a Conference | 34 |
| 4.2.1 Joining a Conference Using the Conference Access Number..... | 34 |
| 4.2.2 Joining an HD Video Conference over an IMS Network..... | 36 |
| 4.2.3 Joining a Third-Party Cloud Video Conference | 40 |
| 4.3 Controlling a Conference | 41 |
| 4.4 Starting Presentation | 49 |
| 4.5 Setting the Answering Mode..... | 50 |
| 4.6 Muting the Local Microphone After Answering a Call | 50 |
| 4.7 Using the Do-Not-Disturb Function | 51 |
| 5 Device Control..... | 52 |
| 5.1 Controlling Cameras | 52 |
| 5.1.1 Using the Remote Control | 52 |
| 5.1.2 Using the Web Interface..... | 53 |
| 5.2 Selecting Video Sources | 54 |
| 5.3 Setting Preferred Video Parameters | 55 |
| 6 Address Book Management..... | 57 |
| 6.1 Adding Sites Using the Web Interface | 57 |
| 6.2 Adding Groups Using the Web Interface | 59 |
| 6.3 Modifying or Deleting Sites or Groups in the Address Book Using the Web Interface..... | 60 |
| 6.4 Importing and Exporting Address Book | 61 |
| 7 System File Management | 62 |
| 7.1 Importing and Exporting Settings..... | 62 |
| 7.2 Backing Up Settings | 63 |
| 7.3 Creating and Downloading a CSR File..... | 63 |
| 8 Operation UI Customization | 65 |
| 8.1 Customizing the Web Interface..... | 65 |

| | |
|---|-----------|
| 8.1.1 Desktop Icons | 66 |
| 8.1.2 Shortcut Bar Icons | 66 |
| 8.2 Customizing the Remote Control UI | 67 |
| 9 Routine Maintenance | 68 |
| 9.1 Maintenance Items | 68 |
| 9.2 Checking the Indicator Status | 69 |
| 9.3 Checking the Operating Environment | 69 |
| 9.4 Checking the Cleanliness | 70 |
| 9.5 Checking the Connection Status | 71 |
| 9.6 Checking Alarms | 71 |
| 9.7 Checking the System Status | 71 |
| 9.8 Checking the System Information | 72 |
| 9.9 Backup and Restoration | 73 |
| 9.10 Restoring Factory Settings | 74 |
| 10 Security Maintenance | 76 |
| 10.1 Overview | 76 |
| 10.1.1 Purpose of Security Maintenance | 76 |
| 10.1.2 What Is Layered Security Maintenance | 76 |
| 10.2 Application Layer Security | 77 |
| 10.2.1 Application Layer Account List | 77 |
| 10.2.2 Restoring Systems to Default Settings | 86 |
| 10.2.3 Configuring Encryption | 87 |
| 10.2.4 Web Management Users | 87 |
| 10.2.5 Web Access Control | 88 |
| 10.2.6 SSH Access Control | 89 |
| 10.2.7 Viewing Logs | 90 |
| 10.2.8 Enabling FTPS | 91 |
| 10.2.9 Configuring an FTPS Server | 91 |
| 10.2.10 Managing Certificates | 94 |
| 10.2.11 Importing and Updating Web Certificates | 95 |
| 10.2.12 Importing and Exporting Settings | 96 |
| 10.3 System Layer Security | 97 |
| 10.4 Network Layer Security | 97 |
| 10.5 Management Layer Security | 98 |
| 10.5.1 Principles of System Maintenance Security | 99 |
| 10.5.2 Guidelines for Password Security Maintenance | 99 |
| 10.5.3 Log Maintenance Suggestions | 99 |
| 10.5.4 Guidelines on Signaling Diagnosis | 100 |
| 10.5.5 Security Evaluation Recommendations | 100 |
| 10.5.6 Backup Suggestions | 100 |
| 10.5.7 Defect Feedback Suggestions | 100 |

| | |
|---|------------|
| 10.5.8 Common Measures Against Attacks | 100 |
| 10.5.9 Security Emergency Response Mechanism | 101 |
| 10.5.10 Security Emergency Response Mailbox | 101 |
| 11 Troubleshooting | 102 |
| 11.1 Fault Diagnosis | 102 |
| 11.1.1 Fault Diagnosis Model | 102 |
| 11.1.2 Fault Diagnosis Methods | 103 |
| 11.2 Common Faults | 106 |
| 11.2.1 Web Interface | 106 |
| 11.2.2 Network | 107 |
| 11.2.3 Video | 108 |
| 11.2.4 Audio | 111 |
| 11.2.5 Conference Initiation | 112 |
| 11.2.6 Conference Control | 114 |
| A Icons on the Remotely Controlled UI | 116 |
| B Requirements on Room Layout and Lighting | 118 |
| C Default Accounts | 119 |
| D Safety Precautions | 121 |
| E Glossary | 126 |

1 Administrator Guidelines

1.1 Application Scope

This document provides guidance for enterprise administrators to perform routine operations.

Enterprise administrators are management and maintenance personnel who are responsible for proper running of the endpoint. They need to perform the following tasks:

- Answer questions posed by enterprise users.
- Perform routine system operations.
- Routinely maintains the endpoint.
- Troubleshoots the endpoint failures.

1.2 Requirements on an Administrator

As an administrator, you must meet the following basic endpoint administrator proficiencies and be capable of collecting all information related to the endpoint and its working environment.

1.2.1 Basic Knowledge

- SC(Switch Center) and Session Initiation Protocol (SIP) servers
- H.323 and SIP protocols
- Ethernet, TCP/IP, and Client/Server (C/S) model
- Safe and effective use of electronic devices
- Common maintenance tools
- Videoconferencing endpoint functions and services



NOTE

The endpoint is restricted to indoor use..

1.2.2 Environment and System Information

Table 1-1 lists the endpoint and working environment information that must be collected, which helps you fulfill your job responsibilities and check the preparations for a recovery from an emergency.

Table 1-1 Information to be collected

| Category | No. | Item | Description |
|---------------------|-----|---|---|
| Device information | 1 | Device location | Record the endpoint location in as much detail as possible so the endpoint can be quickly located. |
| | 2 | Networking condition | Record the network topology and hardware connection diagram that include every device. |
| | 3 | Endpoint information | List the IP address, user name, and password for the endpoint so you can quickly log in to the endpoint in case of an emergency. If you are not permitted to record the password for security reasons, memorize it. |
| Software and tools | 4 | Software versions and tools | List the software versions corresponding to the endpoint. Prepare troubleshooting tools. |
| Contact information | 5 | Purchased parts' service information | Record the manufacturer contact information, serial numbers, and manufacturers' warranty clauses for purchased parts. |
| | 6 | Technical support personnel's contact information | Maintain a list of technical support personnel with their contact information and responsibilities. |
| Spare parts | 7 | Spare parts | List all spare parts (including the spare parts that Huawei can provide) and corresponding procurement methods. |
| | 8 | Redundant or temporary devices | List all redundant or temporary devices in the system, such as standby file servers and database servers. |

1.2.3 Reference Documents

The documents listed in Table 1-2 can help enterprise administrators perform routine operations and maintenance as well as answer questions from common users.

Table 1-2 Reference documents

| Document | Description | When to Use | How to Obtain |
|--|--|---|--|
| TE20 Videoconferencing Endpoint V500R003C00 Quick Installation Guide | Describes the packing list of the endpoint, and the ways to quickly install and configure it. Describes the | When checking whether the carton contains all the required items and when installing the endpoint | To obtain the documentation of a product, visit http://support.huawei.com/enterprise/ and search for product name + version number , for example TE20 V500R003C00 . |


| Document | Description | When to Use | How to Obtain |
|---|--|---|---|
| | packing list and quick installation and configuration methods of the endpoint. | | |
| TE20 Videoconferencing Endpoint V500R003C00 Quick Operation Guide | Describes the commonly used operations on the remote control UI of the endpoint. | When answering questions from common users who are using the endpoint for the first time or unfamiliar with the endpoint | |
| TE20 Videoconferencing Endpoint V500R003C00 Administrator Guide (this document) | Describes routine operations and maintenance on the endpoint. | When answering questions that common users encounter during daily operation | |
| TE20 Videoconferencing Endpoint V500R003C00 Help | Describes the endpoint web interface and method for using this interface. | When answering questions that common users encounter on the endpoint web interface or explaining the parameters on this interface | Log in to the endpoint web interface and click the Help tab. |

1.3 How to Obtain Help

When you encounter an endpoint issue, use the help on the endpoint web interface or contact technical support personnel.

Viewing the Help on the Endpoint Web Interface

- The help on the endpoint web interface includes context-sensitive help and operation guide.
- Context-sensitive help includes status icons and configuration verification messages. For example, if certain settings on the system settings screen are incorrect, a message will be displayed to indicate the error and how to rectify it.

- The operation guide describes how to operate the endpoint web interface. When you are using the endpoint and the documents delivered with the endpoint are unavailable, you can click  in the upper right corner to read the operation guide.

Obtaining Technical Support

The enterprise technical support website is an efficient and real-time communication platform where you can obtain technical documents, submit technical questions, service requests, and troubleshooting questions, and provide feedback on Huawei products. To seek technical help over the Internet, please visit <http://e.huawei.com>.

Provide the following information to help Huawei engineers answer your questions:

- Endpoint serial number (web interface query path: **Help > Version**)
- Software version (web interface query path: **Help > Version**)
- Network information (web interface query path: **Maintenance > System Status > Line Status**)
- Diagnostic and troubleshooting measures you have taken

2 Getting Started

You can clearly know how to log in to the web interface and use the remote control by reading this section.

2.1 Understanding the Remote Control

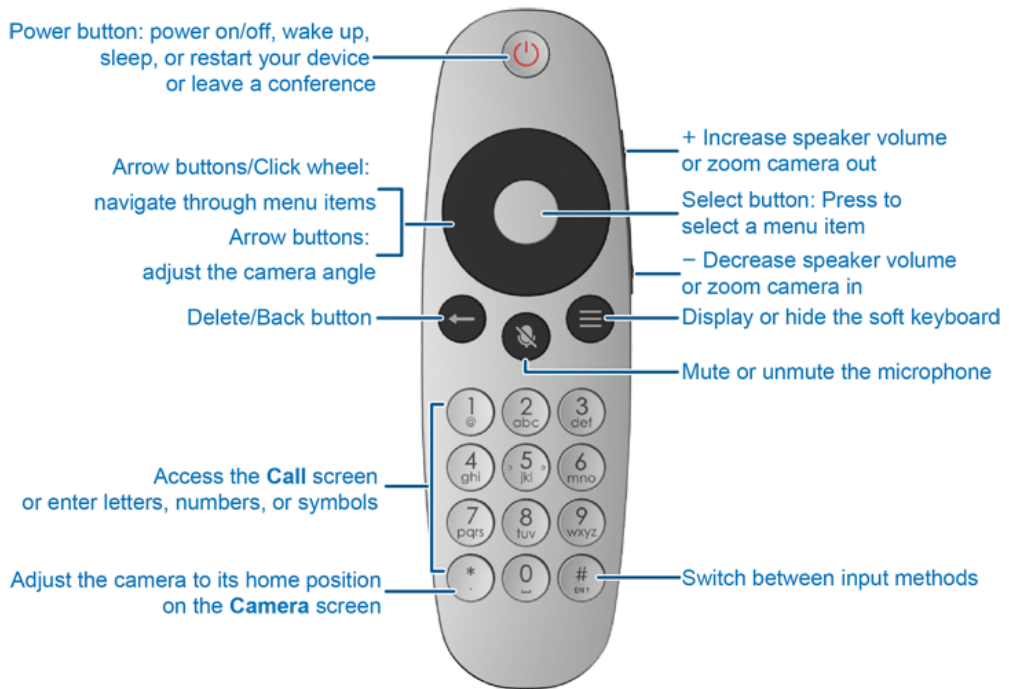
2.1.1 Background

You can use the remote control to easily perform operations such as joining or controlling a conference, modifying system settings, adjusting the camera angle, and setting the layout.

2.1.2 Remote Control Buttons

Figure 2-1 shows what the remote control looks like and the functions of all its buttons.

Figure 2-1 Remote control buttons

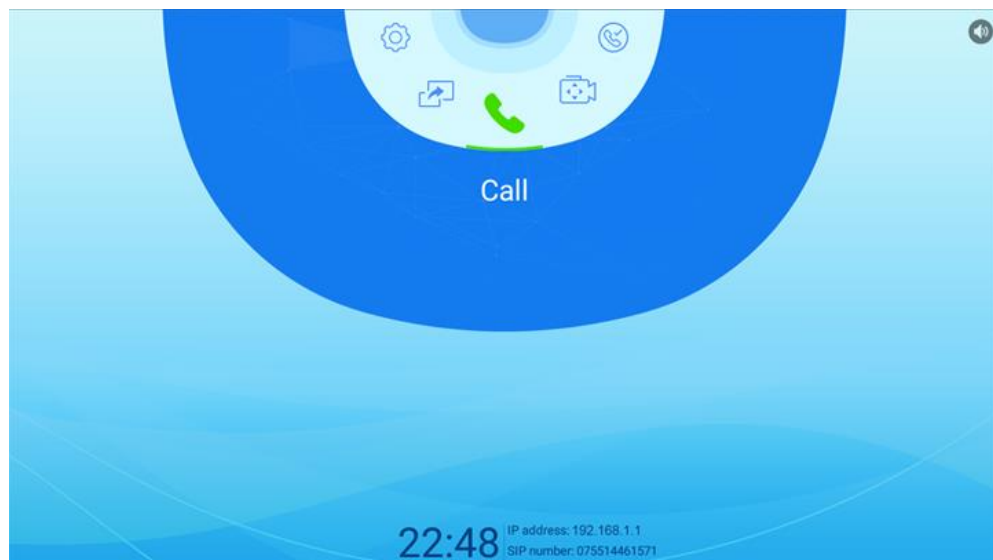





2.1.3 Remote Control UI

This section describes the main menu screen of the remote control UI.

Power on the endpoint and its connected display. You will see the screen shown in Figure 2-2.

Figure 2-2 Main menu screen



- On the main menu, press the  button on the remote control, switch to , and press the  button on the remote control to enter the **Call** screen.
This screen provides two options: **Call** and **Call History**.
- On the main menu screen, you can go between **System Settings**, **AirPresence**, **Call**, **Camera Control** and **Do Not Disturb** using the arrow buttons or click wheel.
 - If you want to access the **System Settings**, enter the password (default: **12345678**).
 - If no administrator password is set beforehand, you can access any module of the remote control UI.



2.1.4 Unpairing a Remote Control

If you want to use a TE10-paired remote control to operate a TE20, unpair the remote control from its paired TE10 first.

The TE10 remote control can be used by the TE20, and vice versa. If you want to use a TE10-paired remote control to operate a TE20, unpair the remote control from its paired TE10 first.

NOTE

It is recommended that you operate the TE10 or TE20 with the remote control that comes with it.

Press and hold the  and  buttons simultaneously for 3s. The unpairing succeeds when you see the remote control indicator on for 1s.

2.1.5 Using the Simulated Remote Control

You can invoke the simulated remote control on the web interface and click on it to control your endpoint.

On the web interface, choose **Device Control** > **Use Remote Control** to invoke the simulated remote control show in Figure 2-3.

Figure 2-3 Simulated remote control



2.1.6 Using a Keyboard or Mouse

You can connect a wired or wireless keyboard or mouse to your endpoint through the USB port. Then you can use it to operate your device just like a remote control.

Using a Keyboard

You will see the screen shown in Figure 2-2 after connecting your endpoint to a wired or wireless keyboard.

Table 2-1 shows the remote control buttons and the keyboard buttons with the same functions.

NOTE

- You can use the keyboard button combinations of the Android operating system to operate the remote control UI. If you want to know functions of these button combinations, visit the Android website.
- The TE20 remote control UI provides a soft keyboard, which is available even though a physical keyboard is connected.

Table 2-1 Remote control buttons and corresponding keyboard buttons

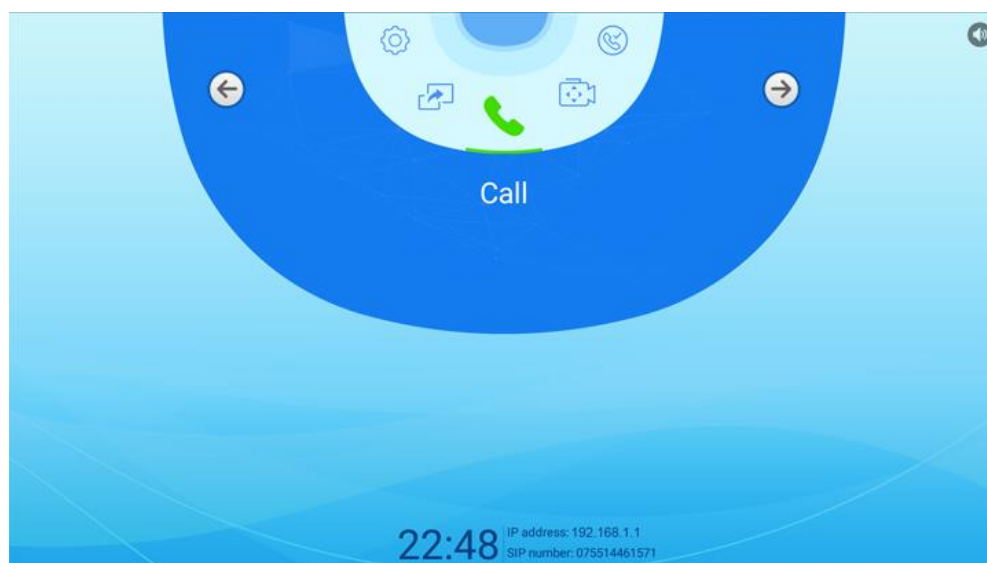
| Remote Control Button | Keyboard Button |
|-----------------------|--|
| Arrow buttons | Arrow buttons |
| Delete button | Delete or Backspace button |
| Back button | Esc button |
| OK button | Enter button |
| Zoom out | Plus (+) button on the numeric keypad |
| Zoom in | Minus (-) button on the numeric keypad |

| Remote Control Button | Keyboard Button |
|------------------------------------|------------------------------------|
| Letter, number, and symbol buttons | Letter, number, and symbol buttons |




Using a Mouse

You will see the screen shown in Figure 2-4 after connecting your endpoint to a wired or wireless mouse.



Figure 2-4 Main menu screen (a mouse connected)



You can use the mouse as follows:

- Click  or  to navigate to a menu item.
- Click a menu item to access its screen. For example, click the  icon to access the **Call** screen.

Then you can perform the following operations:

- Click  or  to go back to the previous screen.
- Click the text box to invoke the soft keyboard. Then use the soft keyboard to enter letters, numbers, or symbols.

NOTE

If a wireless keyboard and mouse suite is connected, you can also use the physical keyboard to enter what you want after a click on the text box.

- On the **Camera** screen, click , , , and  to rotate the camera or click  or  to adjust the focal length.

2.2 Understanding the Web Interface

2.2.1 Background

The endpoint web interface provides users with a wide array of functions, including calling, conference control, address book management, system configuration, and device control. The endpoint web interface enables multiple users to perform operations simultaneously as well as remotely.

2.2.2 Configuring the Browser

Before using the endpoint web interface for remote management, configure the web browser on your computer.

Background

The web interface can run on Microsoft Internet Explorer, Mozilla FireFox, and Google Chrome. Microsoft Internet Explorer 11 is recommended. If you use other browsers or versions, the user interface (UI) display may appear slightly different. The web interface will still work as expected.



NOTE

- Before you begin, ensure that the latest patches for the operating system and browser are installed.
- It is recommended that you use Microsoft Internet Explorer 11 or later. Microsoft has stopped maintaining versions earlier than Internet Explorer 11 or releasing patches for them. Using any of the earlier versions may pose security risks.

Procedure

The following description uses Window7 as an example to describe how to configure Microsoft Internet Explorer 11, FireFox 44.0.2 and Chrome 46.0.2490.80 m. The methods for configuring other browser versions are similar.

- Step 1** Start Internet Explorer.
- Step 2** From the Internet Explorer menu bar, choose **Tools > Internet Options**. In the displayed **Internet Options** dialog box, click the **Security** tab.
- Step 3** In the bottom of the tab, click **Custom level**.
- Step 4** In the **Security Settings** dialog box that is displayed, perform the operations as follows:
 1. Set all options under **Downloads** and **Scripting** to **Enable**.
 2. Select **Display mixed content** under **Miscellaneous**.
- Step 5** Click **OK**.
- Step 6** On the **Security** tab, click **Trusted site** and then **Site**.
The **Trusted site** dialog box is displayed.
- Step 7** In the **Add this website to the zone** text box, enter the IP address of your endpoint. Then click **Add**.
- Step 8** Click **Close**.
- Step 9** Click the **Privacy** tab. Move the slider to display the **Medium** level.

Step 10 Click the **Advanced** tab. Select **Use TLS 1.1** or **Use TLS 1.2** under **Settings**.

Step 11 Click **OK**.


The configuration is complete.

----End

 **NOTE**

To ensure that information can be properly displayed, if you choose to skip [Step 6](#) through [Step 8](#), choose **Tools > Pop-up Blocker > Turn Off Pop-up Blocker** from the menu bar of Internet Explorer.

If you use Mozilla Firefox or Google Chrome, set it as follows:

- Click  in the right corner of the Firefox menu bar to open the settings window. Click **Privacy**, select **Accept cookies from sites**, and click **OK**.
- Use the default settings for Google Chrome.

2.2.3 Logging In to the Web Interface

You can remotely manage the endpoint after logging in to the endpoint web interface.

Prerequisites

Before logging in to the web interface, configure your browser. For details, see [2.2.2 Configuring the Browser](#).

Procedure

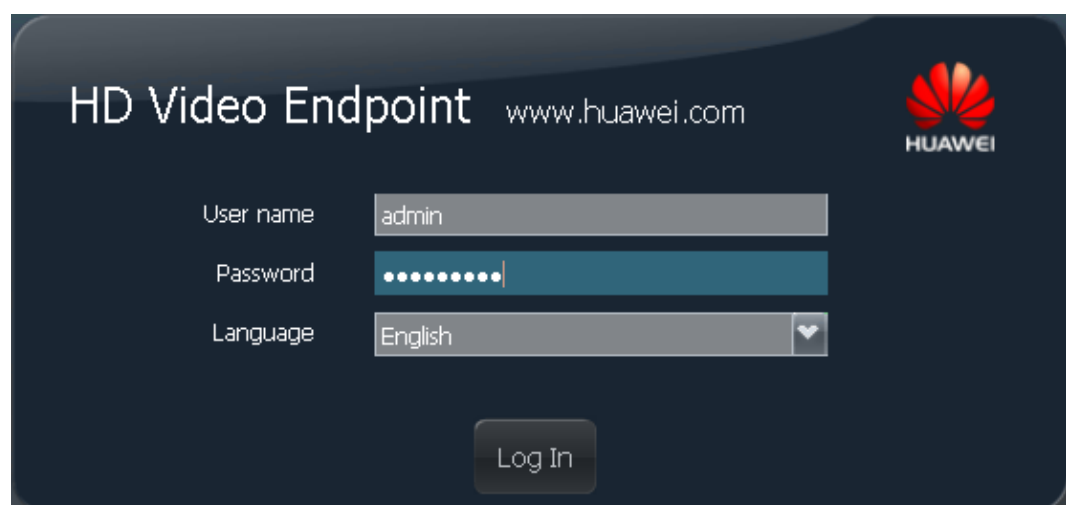
Step 1 Open Internet Explorer.

Step 2 In the address box, enter the endpoint IP address, such as **192.168.1.1**.

Step 3 Press **Enter**.

Log in to the endpoint web interface, as shown in [Figure 2-5](#).

Figure 2-5 Endpoint web login



Step 4 Fill in **User name** and **Password**.

 **NOTE**

The default user name and password are **admin** and **Change_Me** respectively. You are advised to change the default password the first time you log in to the web interface, and then change your password regularly.

Step 5 From the **Language** drop-down list, select a language.

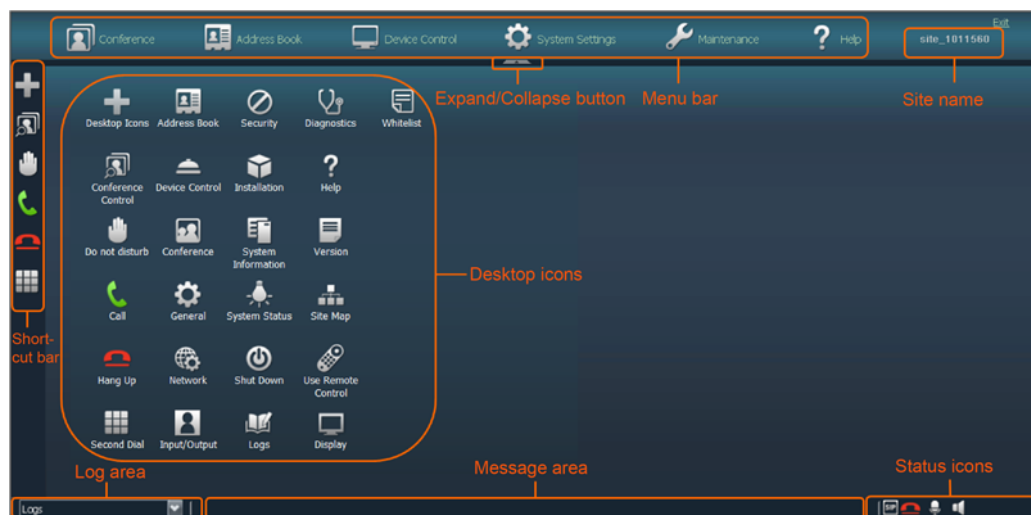
Step 6 Click **Log In**.

The home page is displayed, as shown in Figure 2-6.

 **NOTE**

- To ensure data security, after accessing the endpoint web interface, close the browser and delete browser caches.
- If the computer desktop resolution has been changed, log in to the web interface again.

Figure 2-6 Home page of the endpoint web interface



----End

3 Conference Operations Using the Remote Control

On the remote control interface of the endpoint, you can join a conference in diverse ways. During a conference, you can control the conference, sharing a document, and configure the image layout.

3.1 Initiating a Point-to-Point Conference

You can initiate a point-to-point conference by placing a call to a remote site on the conferencing screen.




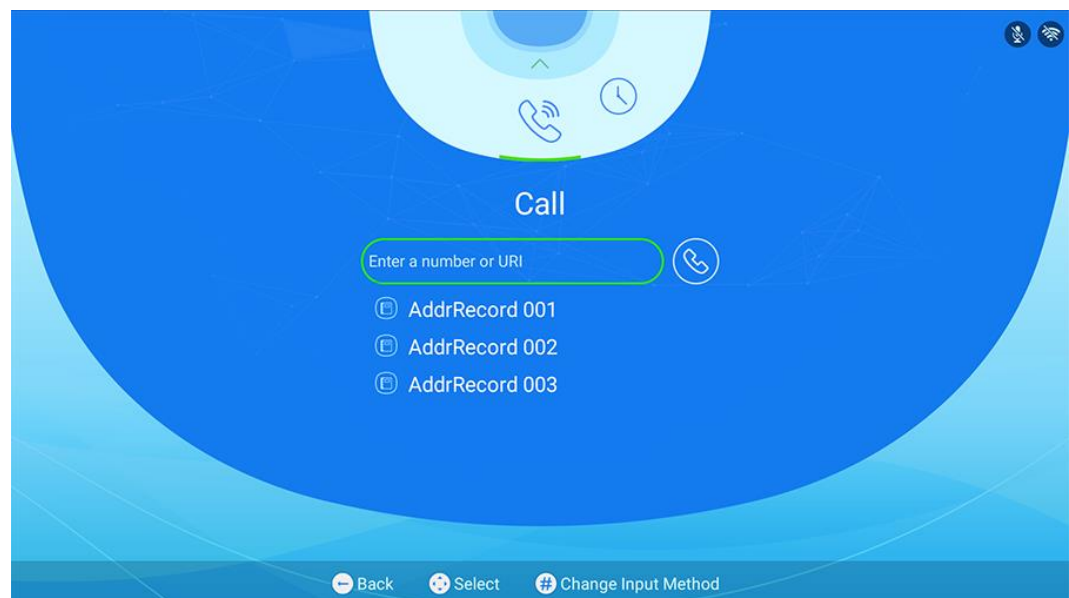



On the main menu, press the  button on the remote control, switch to , and press the  button on the remote control to enter the **Speed Dial** screen, as shown in Figure 3-1.

Figure 3-1 Speed dial



Using the Name, Number, or IP Address of a Remote Site



- Step 1** In the text box on the **Speed Dial** screen shown in Figure 3-1, enter the name, number, or IP address of a remote site.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control to start the conference.
- End

Speed Dial



NOTE

Before placing a call via the address book, create an address book on the web interface by referring to 6 Address Book Management.

- Step 1** On the **Speed Dial** screen shown in Figure 3-1, press the  button on the remote control, and switch to a conference site in the address book.
- If a group is saved in the address book, you need to switch to a conference site under the group.
- Step 2** On the remote control, press the  button to start a conference.
- End

Placing a Call from Your History

The conference history contains the records of conferences your endpoint initiated or attended and sites your endpoint placed calls to or received calls from.



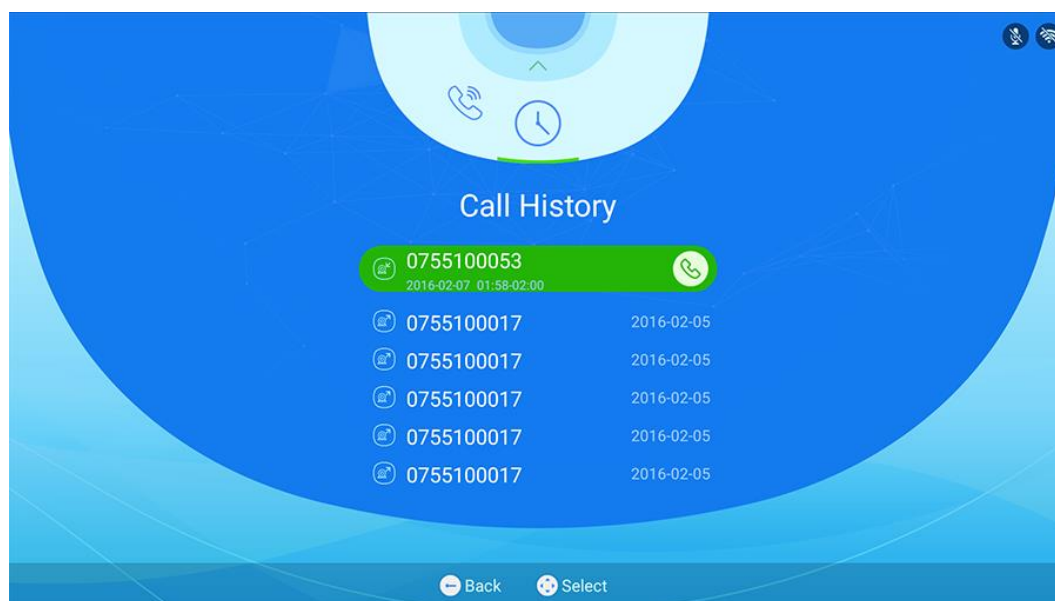

- Step 1** On the **Speed Dial** screen shown in Figure 3-1, press the  button on the remote control, and switch to .
- The **Conference History** page is displayed, as shown in Figure 3-2.

Figure 3-2 Conference history

Step 2 On the remote control, press the  button, and switch to a conference site in the history.

Step 3 On the remote control, press the  button to start a conference.

----End

3.2 Joining a Conference

You can use your remote control to join SMC-based, IMS-based HD, and third-party cloud video conferences.

3.2.1 Joining a Conference by Entering the Conference Access Code

Prerequisites

- You have obtained the conference access number and password (optional) from the conference convener.
- You have set SIP parameters. For details, see *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.

Procedure

Step 1 On the main menu, press any number key on the remote control.

The **Speed Dial** page is displayed, as shown in Figure 3-1.

Step 2 In the text box, enter the conference access number.




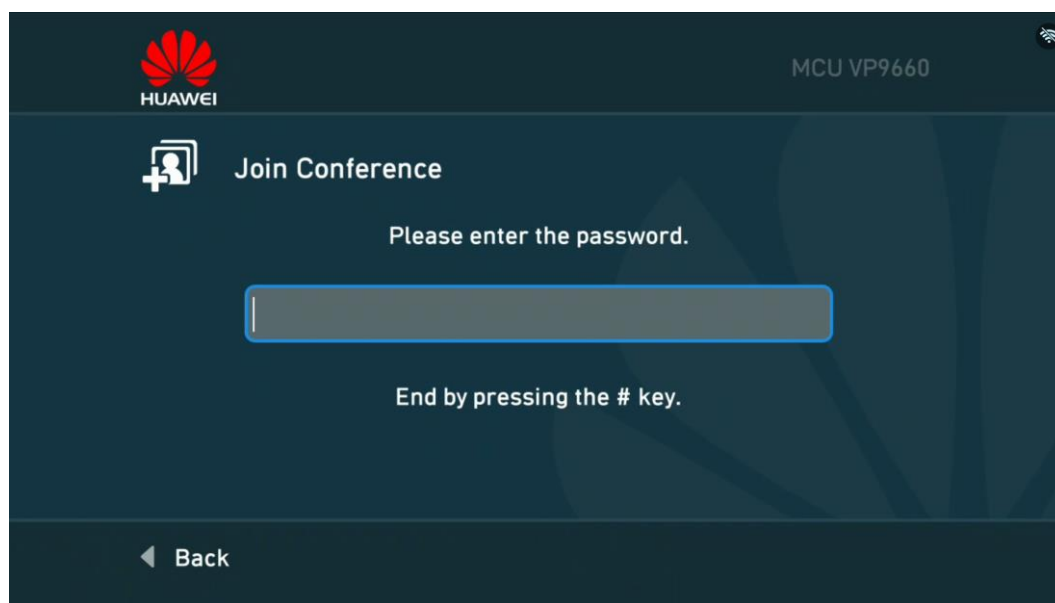
- Step 3** Press the  button on the remote control, switch to , and press the  on the remote control.
- If no password is set for the conference, the endpoint joins the conference directly.
 - If a password is set for the conference, the screen shown in Figure 3-3 is displayed, and continue [Step 4](#) and [Step 5](#).

Figure 3-3 Entering the conference password



- Step 4** Press any number key on the remote control.
The **Two-Stage Dialing** dialog box is displayed.
- Step 5** Enter the conference password and press the # key to join the conference.
----End

3.2.2 Joining an HD Video Conference over an IMS Network

Prerequisites

- You have obtained the conference access number and password (optional) from the conference convener.
- You have set IMS parameters. For details, see [4.2.2 Joining an HD Video Conference over an IMS Network](#).

Procedure

- Step 1** On the main menu, press any number key on the remote control.
The **Speed Dial** page is displayed, as shown in [Figure 3-1](#).
- Step 2** In the text box, enter the conference access number.




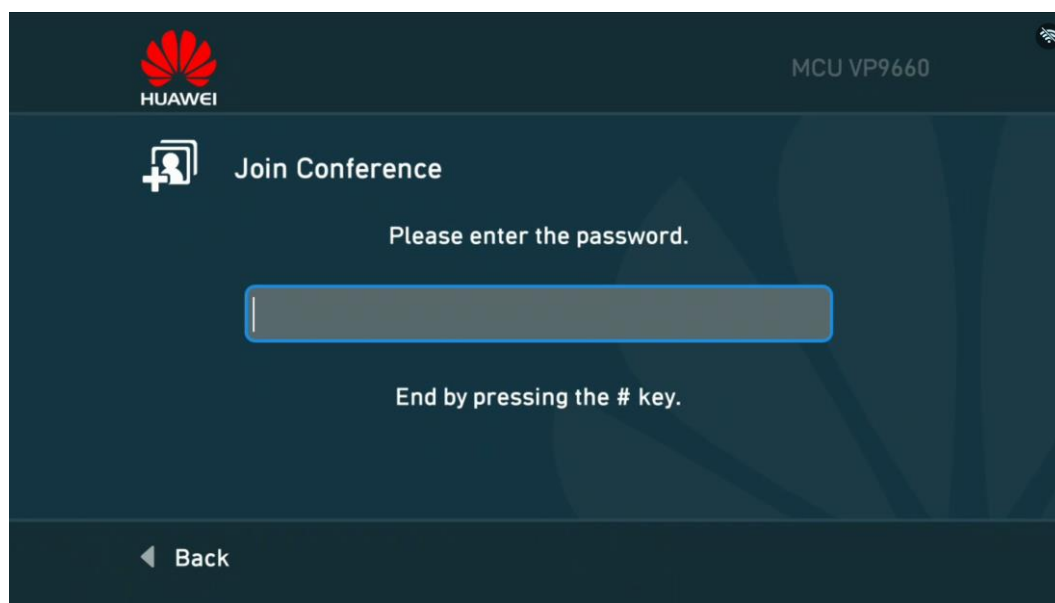
- Step 3** Press the  button on the remote control, switch to , and press the  on the remote control.
- If no password is set for the conference, the endpoint joins the conference directly.
 - If a password is set for the conference, the screen shown in Figure 3-4 is displayed, and continue [Step 4](#) and [Step 5](#).

Figure 3-4 Entering the conference password



- Step 4** Press any number key on the remote control.
The **Two-Stage Dialing** dialog box is displayed.
- Step 5** Enter the conference password and press the # key to join the conference.
----End

3.2.3 Joining a Conference Initiated by a Third-Party Videoconferencing Platform

The endpoint can join HD video conferences initiated by a third-party cloud videoconferencing platform, for example, Videxio cloud videoconferencing platform (referred to as Videxio platform hereinafter).

Prerequisites




- The endpoint has been interconnected with the Videxio platform. For details, see *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.
- A virtual conference room has been set up using the Videxio platform.
- The moderator or guest password for entering the virtual conference room has been obtained from the administrator.

Procedure

Step 1 On the main menu, press any number key on the remote control.

The **Speed Dial** page is displayed, as shown in Figure 3-1.

Step 2 Enter the domain name (example: HUAWEI_TE20.vmr@videxio.com) of a virtual conference room in the text box, or a remote site URI (example: TE20GZ).

Step 3 Press the  button on the remote control, switch to , and press the  on the remote control.

- If no password is set for the conference, the endpoint joins the conference directly.
- If a password is set for the conference, perform operations in [Step 4](#) and [Step 5](#).

Step 4 Press any number key on the remote control.

The **Two-Stage Dialing** dialog box is displayed.

Step 5 Enter a conference password to join the conference.

----End

3.3 Conference Control

Background

In a multi-point conference, you can manage the images and sound of participants.

In a multi-point conference initiated via the MCU (such as VP9660), you can perform conference and site control operations listed in Table 3-1.

 **NOTE**

Operations, including Release Chair, Add Site, Call Site, Mute/Unmute MIC, Broadcast Site, and Disconnect Site, can be performed only after you obtaining chair control rights.



Table 3-1 Conference and site control operations

| | |
|---------------------------|--|
| Conference control | Request Chair, Release Chair, Extend Conference |
| Site control | Add Site, Call Site, Mute/Unmute MIC, View Site, Broadcast Site, and Disconnect Site |

Accessing the Conference Control Screen

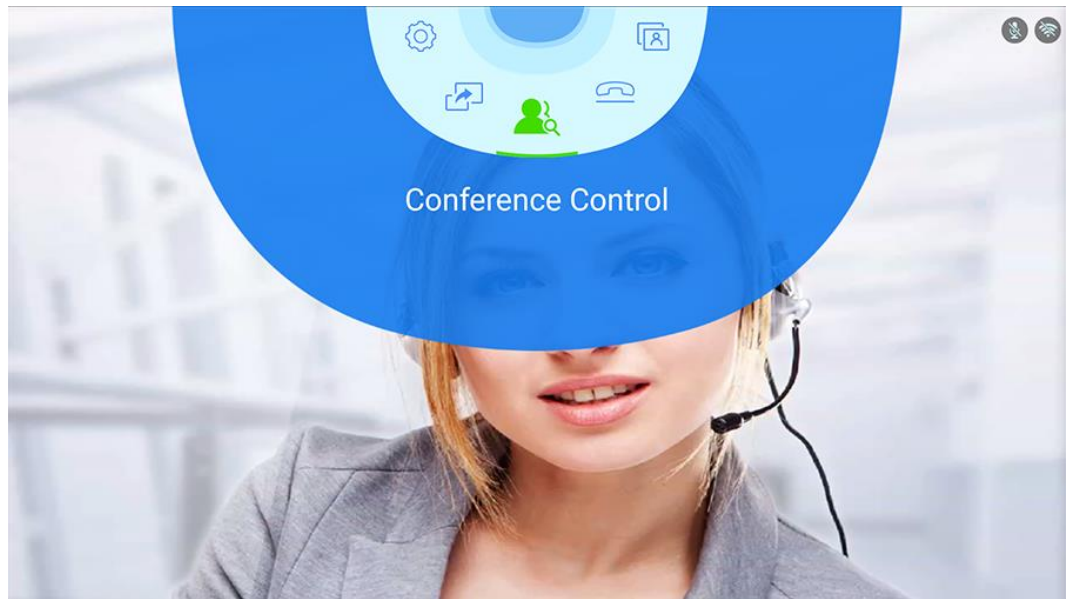
Perform the following operations to access the **Conference Control** screen:

Step 1 To access the menu screen, press the  button on the remote control.

Step 2 Press the  button on the remote control, and switch to .

The conference control page is displayed, as shown in Figure 3-5.








Figure 3-5 Conference control



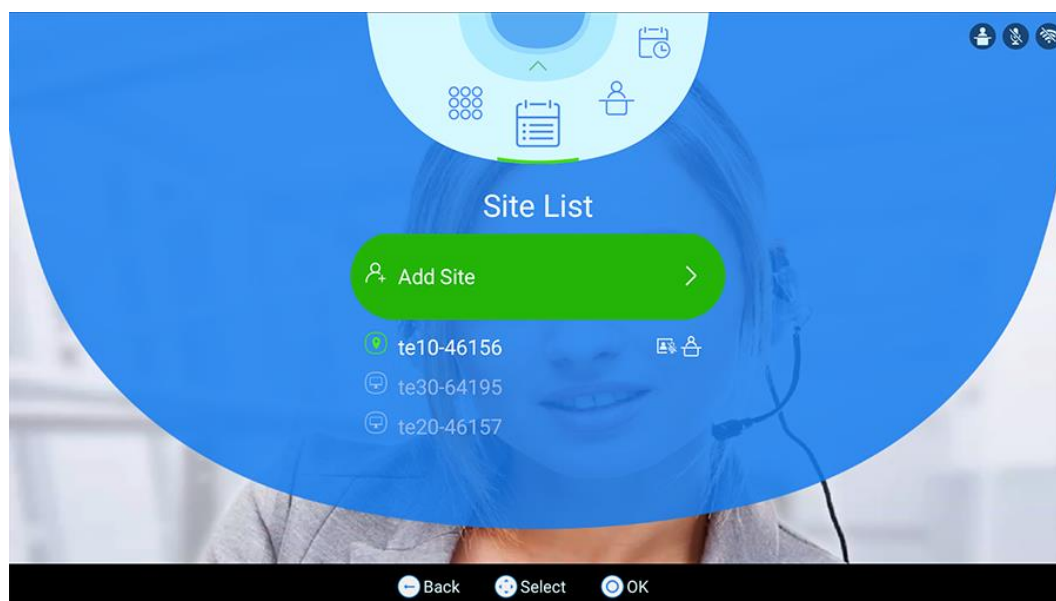
---End

Accessing the Site List Screen

Perform the following operations to access the **Site List** screen:

- Step 1** To access the menu screen, press the  button on the remote control.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.
- Step 3** Press the  button on the remote control, switch to , and press the  on the remote control.

The **Site List** page is displayed, as shown in Figure 3-6.

Figure 3-6 Site list






----End

3.3.1 Request Chair

Application Scenario


Sites can request chair control rights when no chair site exists in a conference. The conference chair site can use more conference control functions than other sites. Audio-only sites cannot request chair control rights.

Procedure

- Step 1** On the **Conference Control** screen shown in Figure 3-5, press the  on the remote control.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.
- Step 3** (Optional) In the text box that is displayed, enter the chair password, choose **OK**, and press the  button on the remote control.

NOTE

Obtain the chair password from the SMC administrator or the site that initiates the conference.

The message **You have successfully obtained chair control rights.** is displayed, and the chair status icon  is displayed in the upper right corner.






----End


3.3.2 Release Chair

Application Scenario

The chair site uses this function to release chair control rights. Other sites can request chair control rights only after chair control rights are released.

Procedure

- Step 1** On the **Conference Control** screen shown in Figure 3-5, press the  on the remote control.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.
- Step 3** Choose **OK** as prompted and press the  button on the remote control.

The message **You have successfully released chair control rights.** is displayed, and the chair status icon  disappeared in the upper right corner.

----End





3.3.3 Extend Conference

Application Scenario

If a conference is not likely to be complete by the scheduled time, the chair site can extend the conference using the **Extend Conference** function.

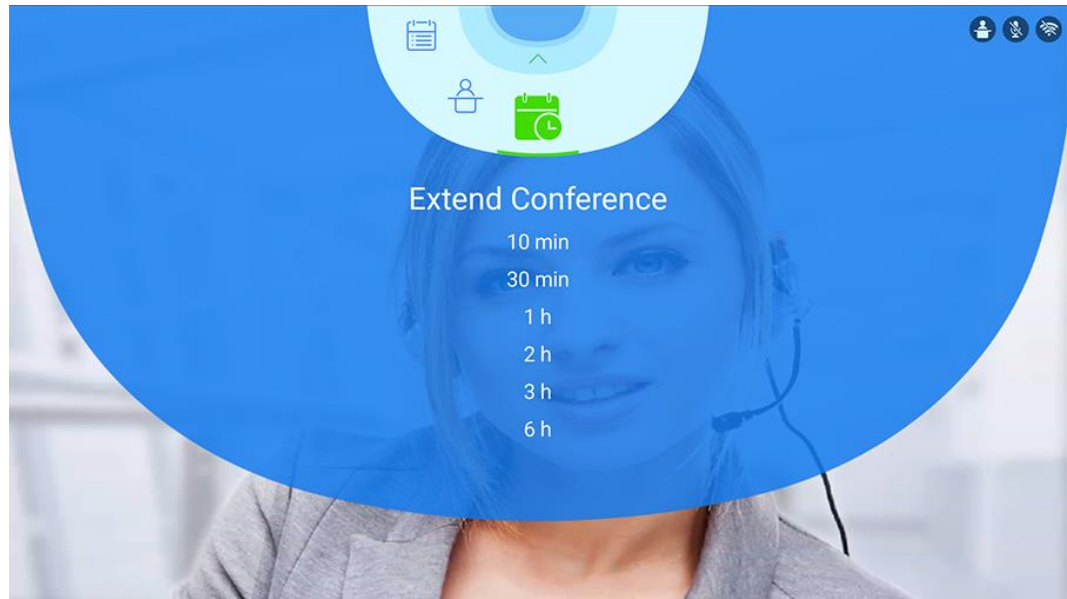
It is recommended that you extend a conference by 30 minutes each time.



Procedure

- Step 1** On the **Conference Control** screen shown in Figure 3-5, press the  on the remote control.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.

The **Extend Conference** page is displayed, as shown in Figure 3-7.

Figure 3-7 Extending a conference



Step 3 Press the  button on the remote control, switch to a time segment, and press the  on the remote control.



----End

3.3.4 Add Site

Application Scenario

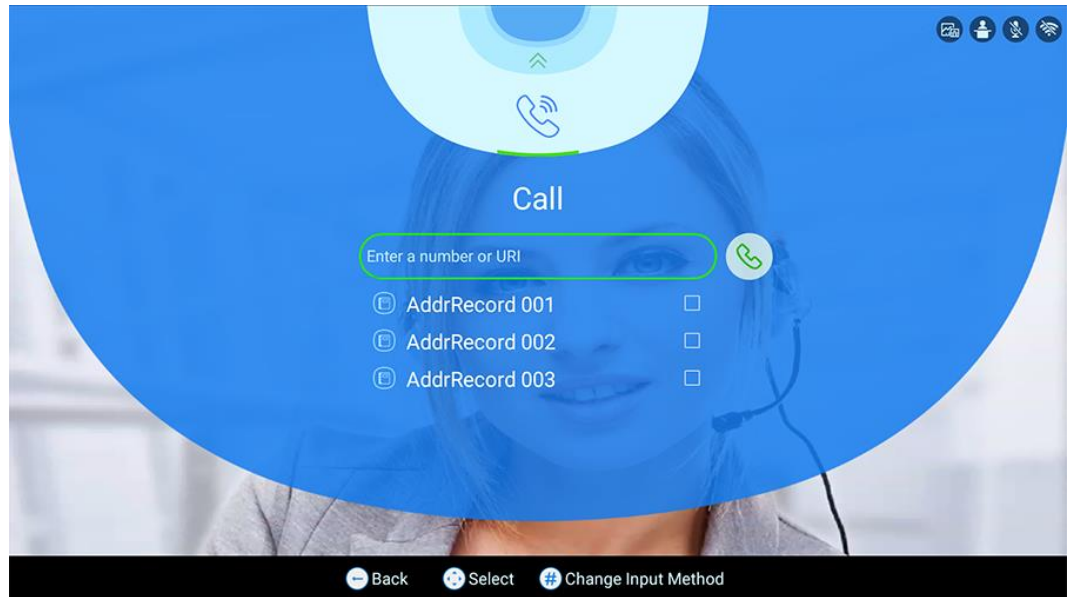
After a conference starts, the chair site can still add sites into the conference. If a site is successfully added to the conference, the site becomes a participant in the conference.

Procedure

Step 1 On the **Site List** screen shown in Figure 3-6, press the  button on the remote control, switch to **Add Site**, and press the  button on the remote control.




The **Speed Dial** page is displayed, as shown in Figure 3-8.

Figure 3-8 Speed dial



Step 2 Press the  button on the remote control and switch to the text box or address book list.

- In the text box, enter the number or IP address of a site you want to add.
- In the address book list, select a site or group you want to add.

Step 3 Press the  button on the remote control, switch to , and press the  on the remote control.


----End



3.3.5 Call Site

Application Scenario

You can place a call to a site that is not in the conference. The site joins the conference after answering the call.

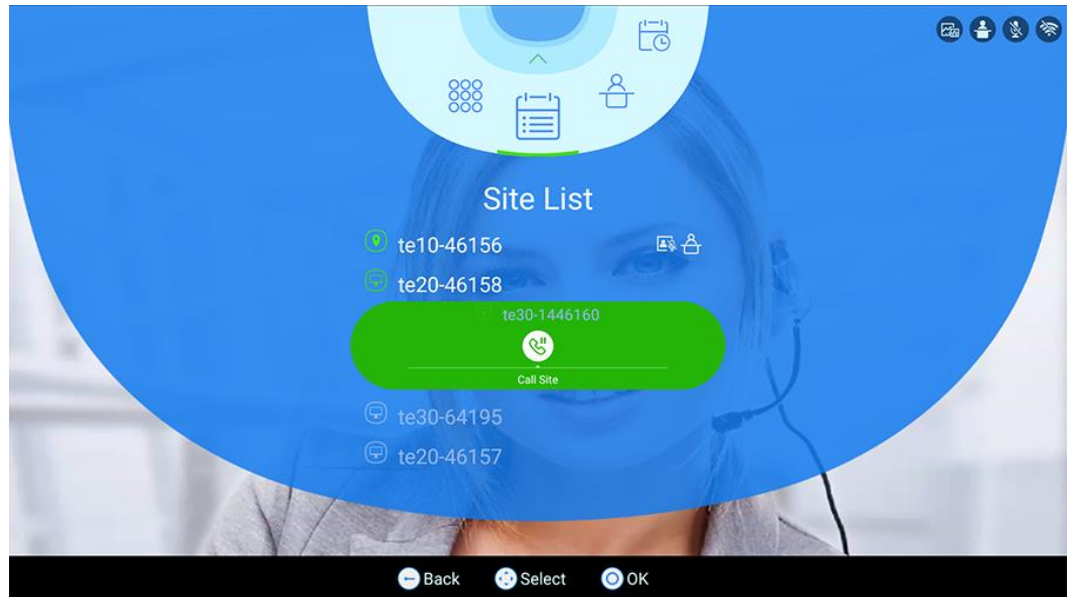
Procedure


Step 1 On the **Site List** screen shown in Figure 3-6, press the  on the remote control.

Step 2 Press the  button on the remote control, switch to a site that has not joined the conference, and press the  on the remote control.

The **Call Site** page is displayed, as shown in Figure 3-9.

Figure 3-9 Calling a site



Step 3 On the remote control, press the  button to start a call.



----End

3.3.6 Mute/Unmute MIC

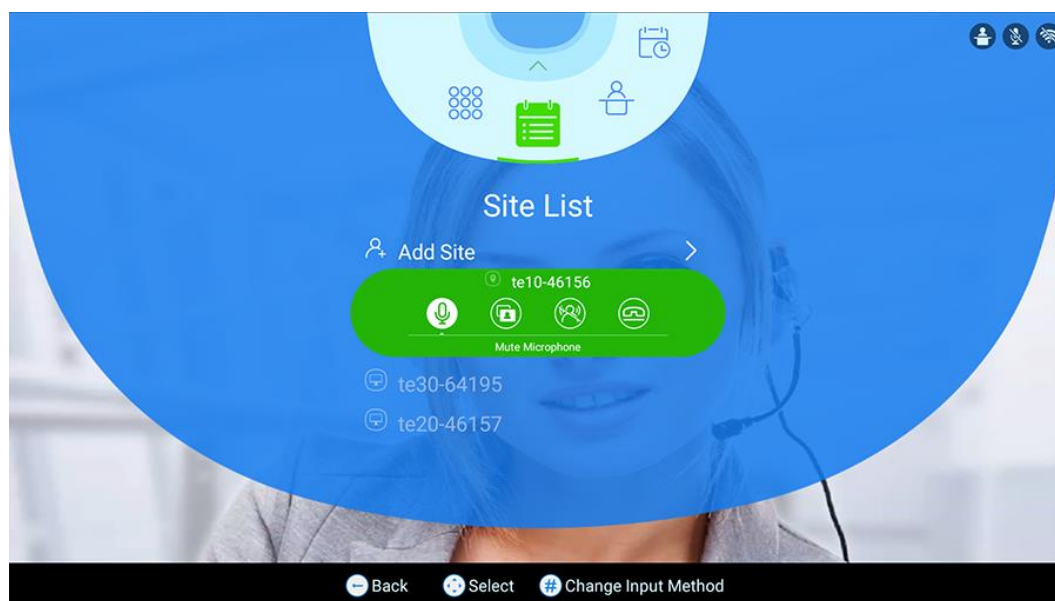
Application Scenario





If the microphone of a site is muted/unmuted by the chair site, the site cannot/can be heard by the other sites.

Procedure

Step 1 On the **Site List** screen shown in Figure 3-6, press the  button on the remote control, switch to a conference site, and press the  button on the remote control.

The conference control page is displayed, as shown in Figure 3-10.

Figure 3-10 Conference control

- Step 2** Press the  button on the remote control, switch to  or , and press the  button on the remote control to mute or unmute the microphone.






----End

3.3.7 View Site

Application Scenario

At your site, you can view continuous presence consisting of multiple sites or view a single site. This operation does not affect the video viewed by other sites.

Procedure

- Step 1** On the **Site List** screen shown in Figure 3-6, press the  button on the remote control, switch to a conference site, and press the  button on the remote control.
- The conference control page is displayed, as shown in Figure 3-10.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.

Watch the video from the conference site.

 **NOTE**

If **Continuous Presence Settings** is set to **Local Presentation**, **View Site** does not take effect.

----End







3.3.8 Broadcast Site

Application Scenario

When a site is broadcast, all non-chair sites (excepting the site being broadcast) are limited to viewing the broadcast site while the chair site can view any site in the conference.

The chair site can broadcast any of the participant sites (except for an audio-only site) in a conference and broadcast multiple sites (including the chair site) in turn at preset intervals.

Procedure







- Step 1** On the **Site List** screen shown in Figure 3-6, press the  button on the remote control, switch to a conference site, and press the  button on the remote control.
- The conference control page is displayed, as shown in Figure 3-10.
- Step 2** Press the  button on the remote control, switch to  or , press the  button on the remote control to start **Broadcast Site** or **Stop Broadcast**.
- End

3.3.9 Disconnect Site

Application Scenario

The chair site can disconnect a site from an ongoing conference. The site then automatically exits the conference. The disconnected site still belongs to the conference. The chair site can invite the site to the conference again using the **Call Site** function.

Procedure





- Step 1** On the **Site List** screen shown in Figure 3-6, press the  button on the remote control, switch to a conference site, and press the  button on the remote control.
- The conference control page is displayed, as shown in Figure 3-10.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.
- Step 3** Press the  button as prompted on the remote control.
- End

3.4 End Conference

Application Scenario

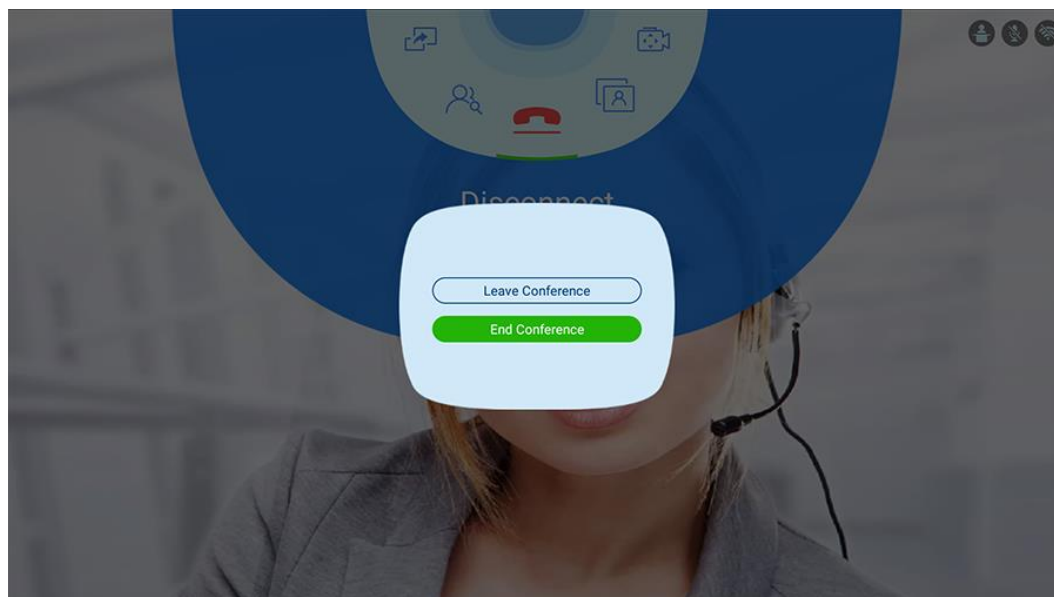
The chair site can end a conference as required.


Procedure

- Step 1** To access the menu screen, press the  button on the remote control.
- Step 2** Press the  button on the remote control, switch to , and press the  on the remote control.

The screen shown in Figure 3-11 is displayed.

Figure 3-11 Ending a conference



- Step 3** Choose **End Conference** and press the  button on the remote control.

 **NOTE**

Choose **Leave Conference**. Only the local site leaves the conference.




----End


3.5 Enabling the Do Not Disturb Function

Application Scenario

If you do not want to be disturbed by incoming calls, you can enable the Do Not Disturb function. After that, no incoming call will be received at your site, and remote sites will be notified that your site is busy when calling you.

Procedure

On the main menu screen, press the  button on the remote control, switch to , and press the  on the remote control.

The  icon is displayed in the upper right corner.

3.6 Starting Presentation

You can share the screen of your computer or mobile device with a remote site.

Prerequisites

- The presentation sharing has been enabled and related parameters have been set. The endpoint enables presentation sharing by default.
To reset parameters, see *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.
- The material source has been connected.
- The AirPresence client cannot be used on a remote desktop.
- For operating system versions that support the AirPresence client, see 4.4 Starting Presentation.



NOTE

Before wireless connections, download and install the AirPresence client by referring to *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.





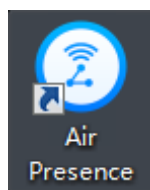


- Wired connection
 - a. Use a cable to connect your computer to the video input interface of the endpoint.
 - b. To access the menu screen, press the  button on the remote control.
 - c. Press the  button on the remote control, switch to , and press the  on the remote control to start the presentation.
If you do not need to share a presentation, choose Stop Sharing on the menu screen.
- Wireless connection
 - a. On your computer desktop, double-click the AirPresence shortcut icon Figure 3-12 to open the AirPresence client.

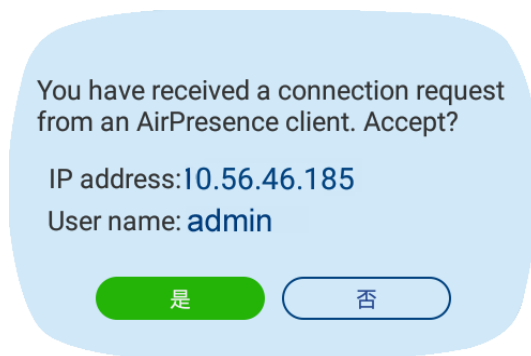
Figure 3-12 AirPresence shortcut icon



- b. Connect the AirPresence client to your endpoint using either of the following methods:
 - In the list of endpoint search results, select an endpoint to connect, and click .
 - Enter the IP address of your endpoint and click .
- c. Start the presentation using either of the following methods:

- In the dialog box that is displayed, enter the AirPresence authentication password and click **Connect**.
The default administrator password is **Change_Me**.
- In the displayed dialog box shown in Figure 3-13, choose **Yes**.

Figure 3-13 AirPresence client request dialog box



If the endpoint is not used in a conference, the computer desktop is shared as a presentation with the endpoint.

If the endpoint is used in a conference, you can click **Share** to send the computer desktop to a remote site.

If you do not need to share a presentation, click Stop Sharing.


When a conference ends, click **Disconnect**.




----End

3.7 Configuring the Conference Screen Layout

You can adjust the screen layout to display a combination of video and presentation.

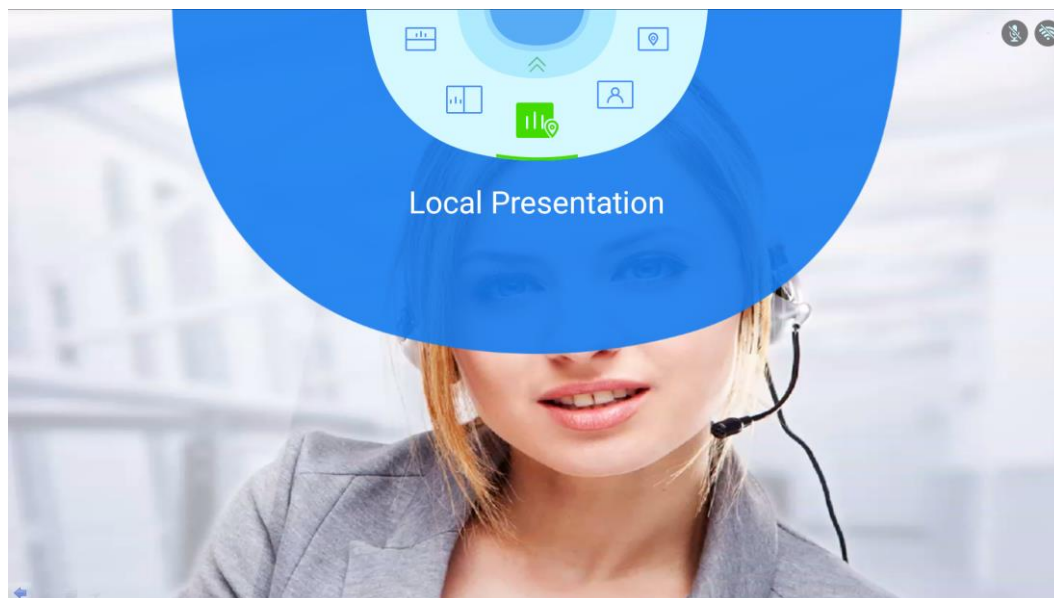
Procedure

Step 1 To access the menu screen, press the  button on the remote control.


Step 2 Press the  button on the remote control, switch to , and press the  on the remote control.



The screen shown in Figure 3-14 is displayed.

Figure 3-14 Example for configuring the conference screen layout



 **NOTE**

Specific icons appearing on the screen layout screen are related to the endpoint status. For example, the **Local Presentation** icon  is displayed only when the local site is connected to a presentation source, and disappears when local presentation is terminated.

Step 3 Press the  button on the remote control, switch to a screen layout model, and press the  on the remote control.

----End



3.8 Adjusting the Volume at Your Site

You can use the remote control to adjust the sound heard by the local site.

Procedure


- Press the plus sign of the volume button on the right of the remote control to increase the sound.
- Press the minus sign of the volume button on the right of the remote control to decrease the sound.


 **NOTE**

- Changing the volume affects only the sound you hear at your site.
- When changing the volume, the status icon  in the upper right corner will change accordingly, and the volume size will be displayed. When the volume is changed to the lowest value, the status icon  will be displayed in the upper right corner.

3.9 Muting or Unmuting the Local Microphone

If you do not want to be heard, mute your microphone.

You can press the  button on the remote control to mute or unmute your microphone.

If your microphone is muted, the  icon will appear in the upper right corner of the remotely controlled UI.



NOTE

The microphone referred to in the section is the local microphone. "3.3.6 Mute/Unmute MIC" is the microphone of any site in a conference. If the chair site mutes a site's microphone, other sites cannot hear that site until the chair site unmutes the site's microphone.

4 Conference Operations Using the Web Interface

You can join conferences in multiple ways on the endpoint web interface. During a conference, you can control the conference or share presentation.

4.1 Initiating a Point-to-Point Conference

You can initiate a point-to-point conference in multiple ways on the endpoint web interface.

4.1.1 Initiating a Conference from the Call Page

On the call page, you can select a site, configure the line type and rate for the site, and place a call to the site to start a conference.

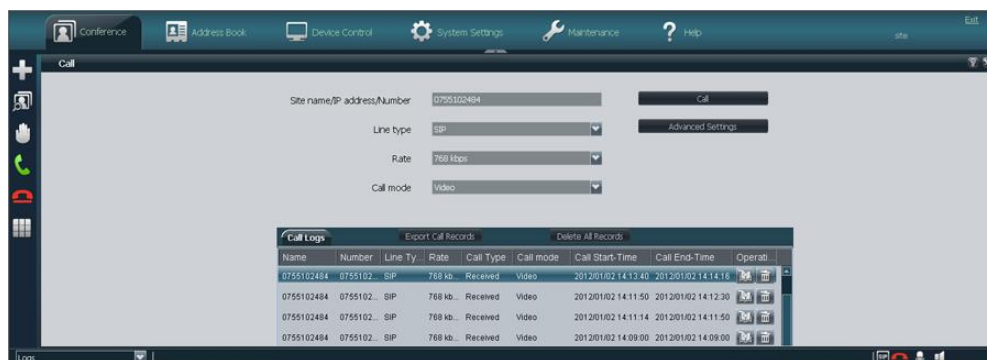
Procedure

Step 1 Choose **Conference > Call**.

Step 2 Select a remote site you want to call using either of the following methods:

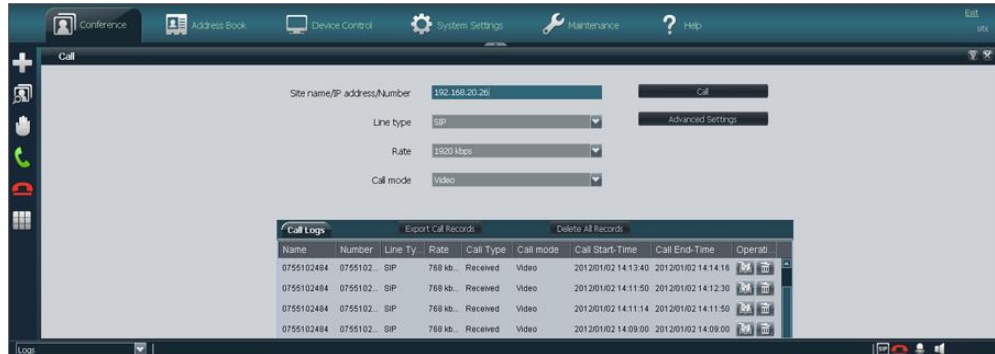
- In the **Call Logs** area, select a remote site, as shown in Figure 4-1.

Figure 4-1 Initiating a call from the call history



- If you do not find your desired remote site in the **Call Logs** window, enter its name, number, URI, or IP address, as shown in Figure 4-2.

Figure 4-2 Initiating a call by site name/number/URI/IP address



Step 3 Set the site parameters listed in Table 4-1.

Table 4-1 Site parameters

| Parameter | Description | Setting |
|-----------------------------|---|---|
| Site name/IP address/Number | Specifies the name, number, URI, or IP address of a remote site. | <ul style="list-style-type: none"> • To call a Cisco TelePresence (CT) site, enter its number. • To call a site on the cloud platform, enter its URI. |
| Line type | Specifies the type of the line used to place the call. | By default, the last used line type is displayed. |
| Rate | Specifies the data transmission rate required. The data transmission rates supported by your endpoint vary depending on the type of site you want to call. | Select the highest available data transmission rate. NOTE If this parameter is set incorrectly, the video quality will be affected or the call might even fail to be set up. |
| Call mode | This parameter is available only after Line type is set to Auto or SIP . The options are as follows: <ul style="list-style-type: none"> • Video: Place video calls. • Voice: Place audio-only calls. | The default value is Video . |

 **NOTE**

The default settings of advanced conference parameters can meet the requirements of most simple conferences. Alternatively, you can click **Advanced Settings** and set advanced conference parameters. For the description of each advanced conference parameter, see *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.

Step 4 Click **Call**.

----End

4.1.2 Initiating a Conference from the Address Book Page

From the address book on your endpoint, you can select sites to initiate a conference.

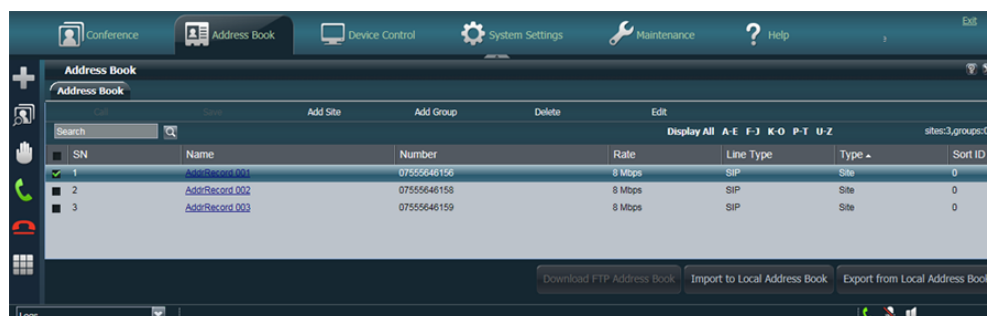
Procedure

Step 1 Choose **Address Book > Address Book**.

Step 2 Choose the site you would like to call from the address book and click **Call**, as shown in Figure 4-3.

You can select an address book record and edit it.

Figure 4-3 Initiating a call from the address book



----End

4.2 Joining a Conference

You can join a conference on the endpoint web interface.

4.2.1 Joining a Conference Using the Conference Access Number

When initiating a conference for which the participant sites are uncertain, you can set only the number of anonymous sites. With this setting, a site can join the conference by dialing the conference access number and then following the interactive voice response (IVR) instructions.

Background

A site dials a conference access number and follows the IVR instructions to enter the specified password to join a conference. This process is called two-stage dialing.

Procedure

Step 1 Obtain the access number for the authentication conference.

- When a conference starts, endpoints that have joined the conference can view the conference access number by choosing **Maintenance > System Status > Conference**.

- Or they can obtain the conference access number and password from the SMC2.0 administrator.

Step 2 Choose **Conference > Call**.

Step 3 In the **Site name/IP address/Number** text box, enter conference access number, for example, 0755100000159.

Step 4 Set the call parameters. Their description is provided in Table 4-1.

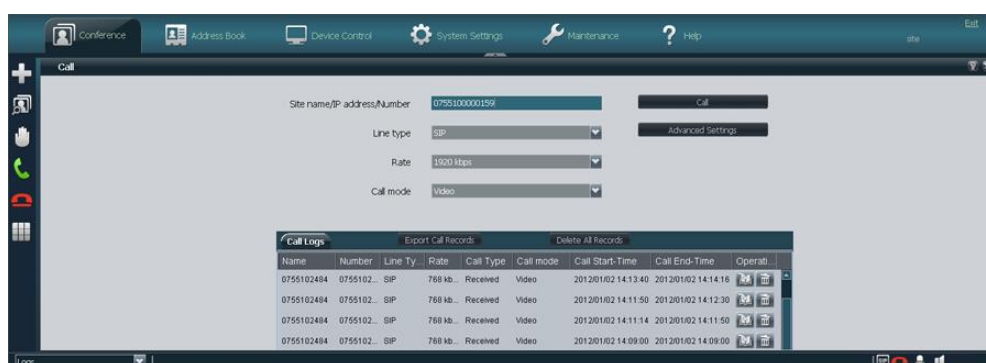


NOTE

Select the highest data transmission rate supported by your endpoint to increase the call success rate.

Step 5 Click **Call**, as shown in Figure 4-4.

Figure 4-4 Entering the conference access number



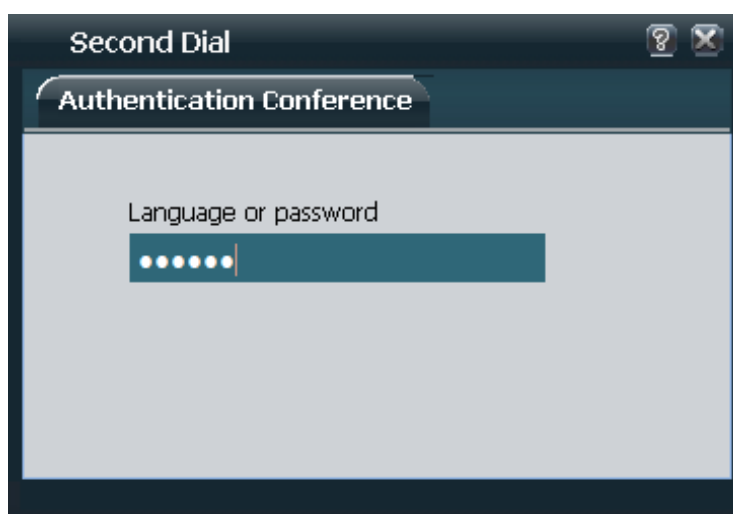
Step 6 Choose **Conference > Second Dial**. Then enter the conference password and press the pound button (#) as prompted, as shown in Figure 4-5.



NOTE

To join a conference that has a password, enter the password using the keypad.

Figure 4-5 Entering the conference password



----End

4.2.2 Joining an HD Video Conference over an IMS Network

The endpoint can join an HD video conference over an IP Multimedia Subsystem (IMS) network.

Background

Borne by the standard IP protocol, IMS uses VoIP applications based on the standard SIP applications of the 3GPP to provide fixed and mobile multimedia services for operators. Integrating MCUs can enhance the functionality of the Huawei IMS HD videoconferencing solution.

Prerequisites

You have obtained the required authentication information from the IMS administrator: unified access number, conference ID, and conference password.



NOTE

The endpoint users can obtain the required authentication information allocated by the IMS through emails, text messages, notices, or other methods.

Procedure

Step 1 Register the endpoint with the network where the IMS is located.

1. On the endpoint web interface, choose **System Settings** > **Network** and click the **H.323/SIP Settings** tab.
2. Under **SIP**, set IMS interconnection parameters listed in Table 4-2 to register your endpoint with the IMS network.

Figure 4-6 Setting IMS interconnection parameters

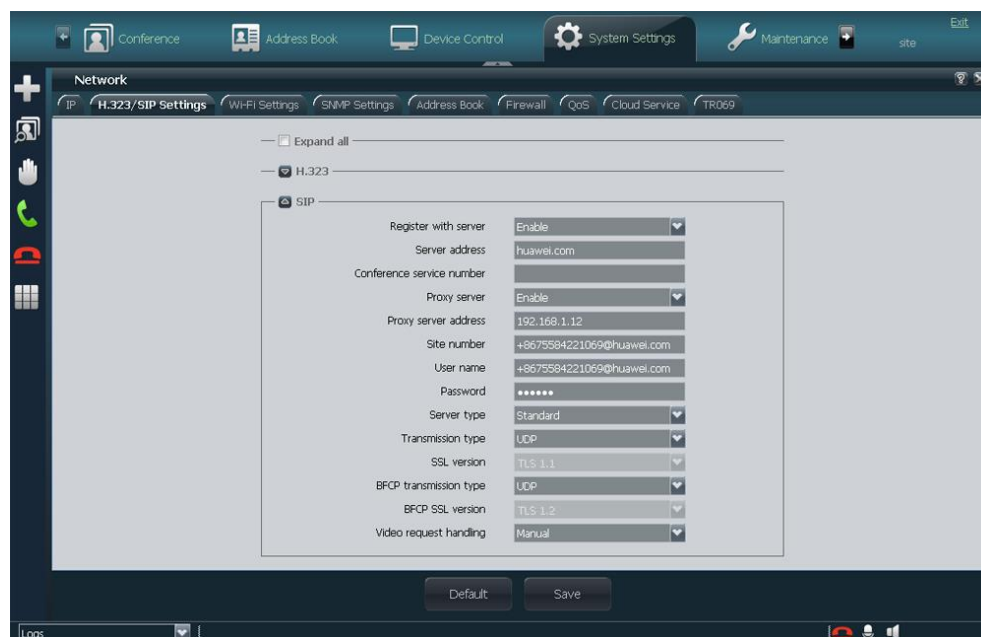



Table 4-2 Parameter description

| Parameter | Description | Setting |
|---------------------------|--|---|
| Register with server | <p>Specifies whether your endpoint registers with an IMS server.</p> <p>Only endpoints that have registered with IMS servers can join the IMS network.</p> <p>An endpoint that registers with an IMS server can place calls to remote sites using their IP addresses or site numbers if the remote sites also register with IMS servers.</p> <p>NOTE</p> <p>If Register with server is set to Enable, you need to set Server address, Conference service number, Site number, User name, and Password.</p> | Set this parameter to Enable . |
| Server address | <p>Specifies the IP address or domain name of the IMS server with which you want the endpoint to register.</p> <p>If you set this parameter to the domain name of the IMS server, enable the domain name server (DNS). If the DNS is not enabled, set Proxy server to Enable to enable it.</p> | <p>IP address example: 192.168.1.10</p> <p>Domain name example: huawei.com</p> <p>It is recommended that you set Server address to the domain name of the IMS server with which you want the endpoint to register.</p> |
| Conference service number | <p>Specifies the conference service number for your endpoint to initiate conferences over an IP multimedia subsystem (IMS) network.</p> <p>Set this parameter to the conference service number obtained from the IMS network administrator.</p> | Leave this parameter empty. |
| Proxy server | <p>Specifies whether to enable the proxy server.</p> <p>You must enable the proxy server when using the IMS network.</p> | Set this parameter to Enable . |
| Proxy server address | <p>Specifies the address of the proxy server.</p> <p>If you set Server address to the IMS server domain name, set this parameter to the IP address bound to that domain name.</p> | Example: 192.168.1.12. |
| Site number | <p>Specifies the site number for your endpoint.</p> <p>If your endpoint registers with an IMS server, endpoints that also register with the IMS server can dial this site number to call your endpoint.</p> | <p>Example: +8675584221069@huawei.com</p> <p>No default value is set for this parameter.</p> <p>The value can contain digits,</p> |

| Parameter | Description | Setting |
|------------------------|--|--|
| | | letters, and special characters, such as @ # %. |
| User name Password | Specify the user name and password that your endpoint uses to register with the IMS server. The password you set here must be the same as that set on the IMS server beforehand. | User name example: +8675584221069@huawei.com Obtain the value of this parameter from the IMS server administrator. |
| Server type | Specifies the SIP server type. <ul style="list-style-type: none"> • Standard: Select this option if your endpoint registers with other SIP servers. • CISCO VCS: Select this option if your endpoint registers with the Cisco TelePresence Video Communication Server (VCS). | Set this parameter to Standard . |
| Transmission type | Specifies the protocol used for SIP signaling transmission. <ul style="list-style-type: none"> • TCP: Use the Transmission Control Protocol (TCP) to implement transmission reliability. • UDP: Use the User Datagram Protocol (UDP) to implement transmission with reduced latency. • TLS: Use Transport Layer Security (TLS) to implement transmission security. With this option selected, a root certificate must be imported when your endpoint registers with a SIP server. For details, see 10.2.10 Managing Certificates. The call rate may be compromised if this option is selected. | Set this parameter to UDP . The IMS network only supports UDP transmission. |
| SSL version | Specifies the encryption protocol used by SIP calls. The value can be TLS 1.0 or TLS 1.1 . NOTE This parameter is available only after Transmission type is set to TLS . | The default value is TLS 1.1 . |
| BFCP Transmission type | Specifies the protocol used for BFCP signaling transmission. <ul style="list-style-type: none"> • Auto: Automatically select a protocol based on the BFCP transmission type supported by the remote site. • TCP: Use the Transmission Control Protocol (TCP) to implement | The default value is UDP . |

| Parameter | Description | Setting |
|------------------------|---|---------------------------------------|
| | <p>transmission reliability.</p> <ul style="list-style-type: none">• UDP: Use the User Datagram Protocol (UDP) to implement transmission with reduced latency.• TLS: Use Transport Layer Security (TLS) to implement transmission security. If you select this option, you can import a root certificate when your endpoint is sharing presentation or during some conferencing operations. For details, see 10.2.10 Managing Certificates. Note that selecting this option may affect the call rate. <p>NOTE The BFCP Transmission type option is available when the imported license file is an encrypted one.</p> | |
| BFCP SSL version | <p>Specifies the encryption protocol used by SIP calls. The options are TLS 1.0, TLS 1.1, and TLS 1.2.</p> <p>NOTE This parameter is available only when BFCP Transmission type is set to TLS.</p> | The default value is TLS 1.2 . |
| Video request handling | <p>Specifies how your endpoint handles video requests from a remote endpoint during a point-to-point SIP audio call or multipoint conference.</p> <ul style="list-style-type: none">• Accept automatically: Your endpoint automatically accepts video requests from the remote endpoint.• Reject automatically: Your endpoint automatically rejects video requests from the remote endpoint.• Manual: Your endpoint prompts you to accept video requests from the remote endpoint. | The default value is Manual . |

3. Click **Save**.

After your endpoint successfully registers with the IMS server, the  icon is displayed in the lower right corner of the web interface.

Step 2 Choose **Conference > Call**.

Step 3 In the text box, enter the conference unified access number.

Step 4 Click **Call**.

Step 5 Choose **Conference > Second Dial**.

Enter the required authentication information, such as the conference ID and password, as prompted.

----End

4.2.3 Joining a Third-Party Cloud Video Conference

The endpoint can join HD video conferences initiated by a third-party cloud videoconferencing platform, for example, Videxio cloud videoconferencing platform (referred to as Videxio platform hereinafter).

Background

The endpoint joins a conference initiated by the Videxio platform by calling the virtual conference room provided by the platform.

Prerequisites

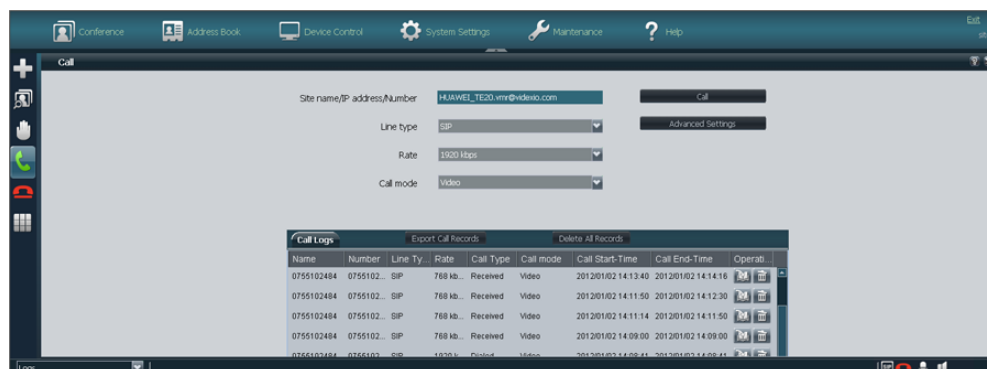
- A virtual conference room has been set up using the Videxio platform.
- The endpoint has been interconnected with the Videxio platform. For details, see *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.
- The moderator or guest password for entering the virtual conference room has been obtained from the administrator.

Procedure

Step 1 On the endpoint web interface, choose **Conference > Call**.

Step 2 Enter the domain name (for example, **HUAWEI_TE20.vmr@videxio.com**) of the virtual conference room in the **Site name/IP address/Number** field to join the conference, as shown in Figure 4-7.

Figure 4-7 Joining a multipoint conference



NOTE

If your desired virtual conference room exists in the **Call Logs** window, directly initiate a call; otherwise, choose **Address Book > Address Book**, search for your desired virtual conference room, and initiate a call.

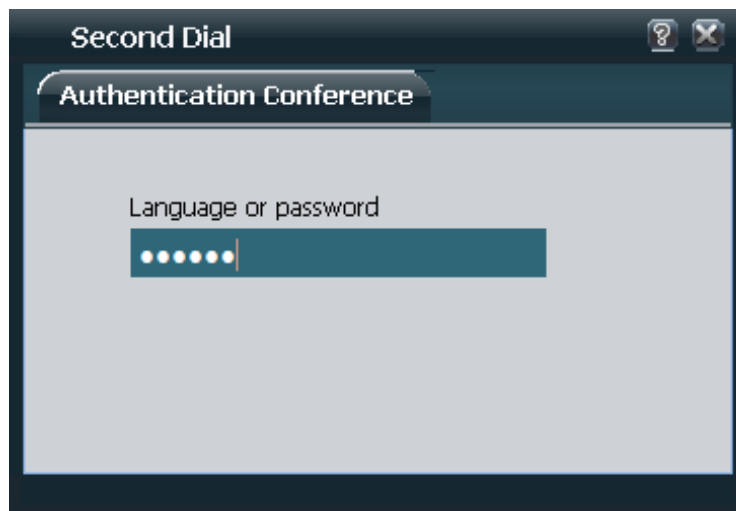
Step 3 Click **Call**.

Step 4 (Optional) Choose **Conference > Second Dial**. Follow the IVR instructions to enter the password to join a conference, as shown in Figure 4-8.

**NOTE**

If the conference has a password, enter the password using the keypad.

Figure 4-8 Entering the password



----End

4.3 Controlling a Conference





After initiating a multipoint conference, you can control the video and audio of sites using conference control functions.

On the web interface, choose **Conference > Conference Control**, and perform conference control operations on the **Conference Control** page.

Icons on the Conference Control Page

Table 4-3 lists common icons displayed on the conference control page.

Table 4-3 Icons on the conference control page

| Icon | Description |
|---|---|
|  | Your site is chairing the conference. |
|  | The conference site is muted, and cannot be heard by other sites. This icon indicates that a site is muted by itself rather than the chair. |
|  | The microphones of the site have been muted, and the other sites in the conference cannot hear the site. |
|  | The microphones of the site have been unmuted, and the |










| Icon | Description |
|---|--|
| | other sites in the conference can hear the site. |
|  | The site is being broadcast. |
|  | The site is being viewed. |
|  | The site is not in the conference. |
|  | The site is in the conference. |
|  | The site is sharing a presentation. |
|  | The site is a H.323 PHONE, or SIP audio site. |

Table 4-4 lists the icons used to adjust the site display mode on the conference control page.

Table 4-4 Icons used to adjust the site display mode

| Icon | Description |
|---|--|
|  | Refreshes the conference control page. |
|  | Displays sites in a list. |
|  | Displays sites as icons. |

Request Chair

Only sites that are not the chair can request chair control rights. The chair site has more conference control rights than non-chair sites. Sites can request chair control rights when no chair site exists in a conference. Audio-only sites cannot request chair control rights.

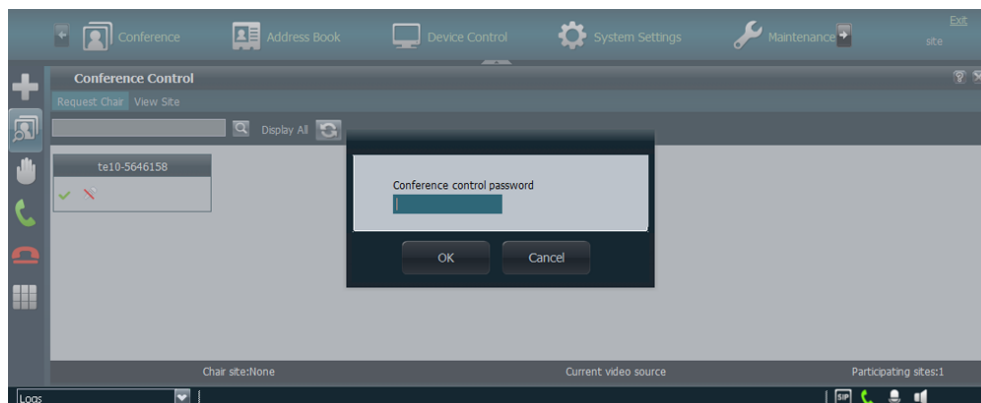
Only one chair site exists in a conference. Other sites can request to be the chair site only after the chair control rights are released or revoked.

Step 1 Click **Request Chair**.


Step 2 (Optional) Enter the conference control password, that is, the chair password, as shown in Figure 4-9.

Obtain the conference control password from the SMC2.0 administrator or the site that initiates the conference.

Figure 4-9 Entering the chair password



Step 3 Click **OK**.

When the  icon is displayed, the site has become the chair site.

----End

Broadcast Site

The chair site can broadcast any video site, including the chair site itself. When a site is broadcast, all non-chair sites are forced to view the video of the broadcast site while the chair site can view the video of any site that is present at the conference.

Step 1 Click **Broadcast Site**.

Step 2 Select a conference site.


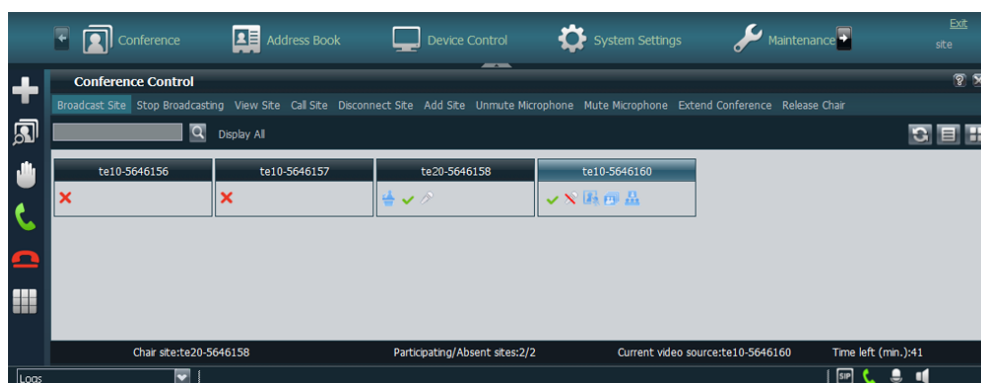
When the  icon is displayed, the conference site has been broadcast, as shown in Figure 4-10.

Figure 4-10 Broadcasting a site



----End

Stop Broadcasting

The chair site can use the **Stop Broadcasting** operation to stop site broadcast. After **Stop Broadcasting** is implemented, all conference sites can watch any other site.

Step 1 Click **Stop Broadcasting**.

Step 2 Select a conference site that is being broadcast.


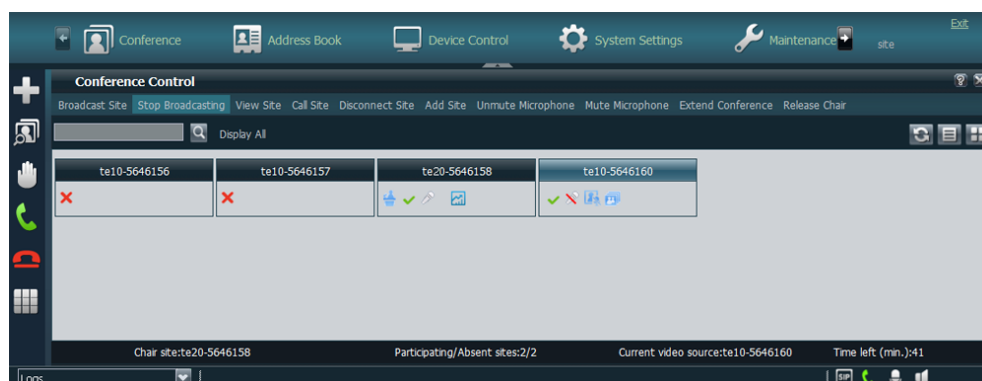
When the  icon disappears, site broadcast has been terminated, as shown in Figure 4-11.

Figure 4-11 Terminating site broadcast



----End

View Site

At your site, you can view continuous presence consisting of multiple sites or view a single site. This operation does not affect the video viewed by other sites.

Step 1 Click **View Site**.

Step 2 Select a conference site.


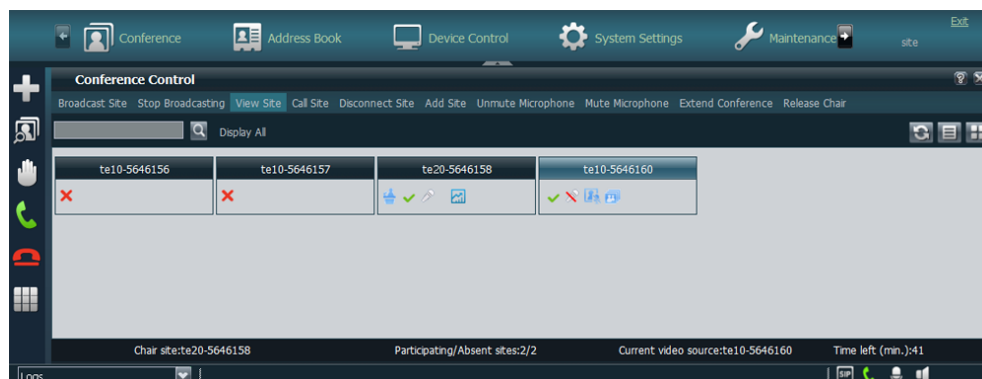
When the  icon is displayed, the conference site is being viewed, as shown in Figure 4-12.

Figure 4-12 Viewing a conference site



----End

Call Site

The chair site can place a call to a site that is not in the conference. The site joins the conference after answering the call.

Step 1 Click Call Site.

Step 2 Select a conference site.


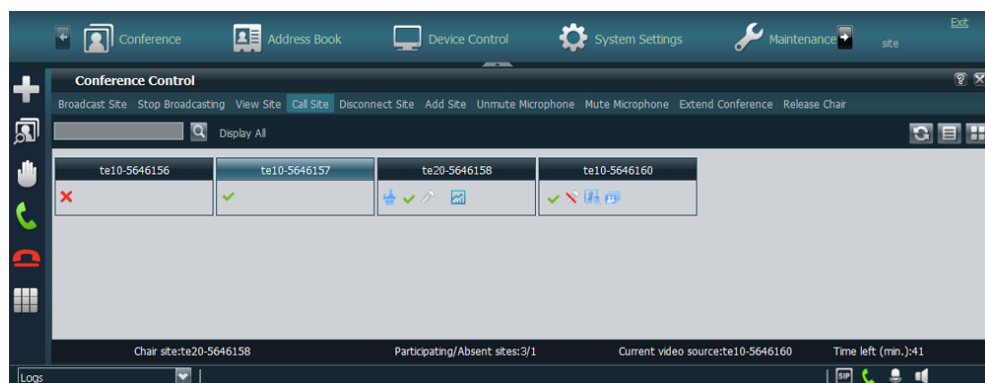
When the  icon is displayed, the conference site has joined the conference, as shown in Figure 4-13.

Figure 4-13 A site that has joined the conference



----End

Disconnect Site

The chair site can disconnect a site from an ongoing conference. The site then automatically exits the conference. The disconnected site still belongs to the conference. The chair site can invite the site to the conference again using the **Call Site** function.

Step 1 Click **Disconnect Site**.

Step 2 Select a conference site.


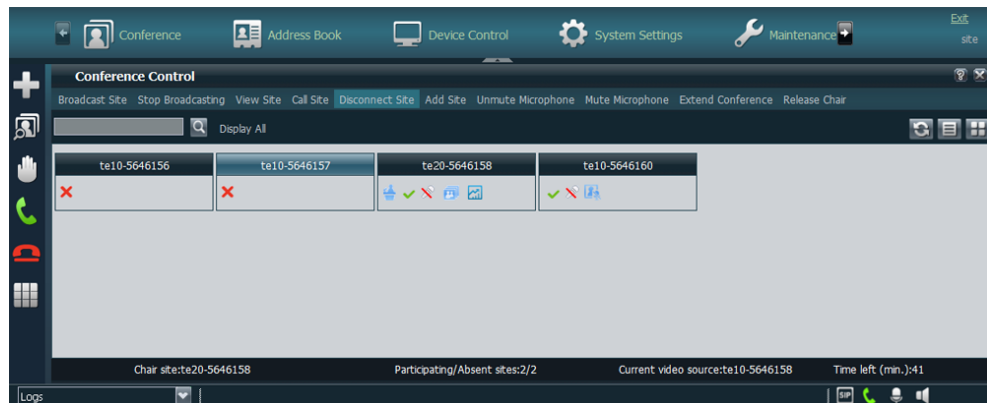
When the  icon is displayed, the conference site has been disconnected, but still exists in the conference, as shown in Figure 4-14.

Figure 4-14 A site that has been disconnected



----End

Add Site

After a conference starts, the chair site can still add sites into the conference. If a site is successfully added to the conference, the site becomes a participant in the conference.

Step 1 Click **Add Site**.

Step 2 To add sites from the local or LDAP address book or add sites that have not been defined in the address book.

Step 3 Click **Add Site**.


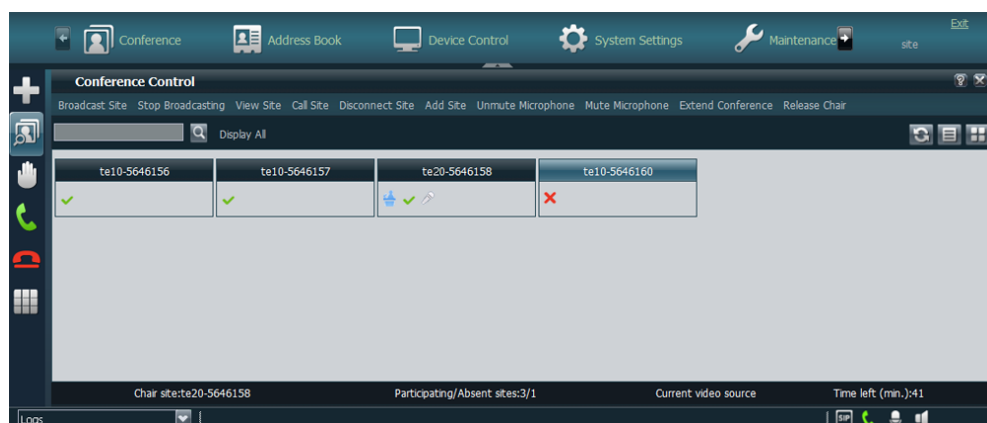
When the  icon is displayed, the conference site has been added to the conference, but has not joined the conference. You can use the **Call Site** function to invite the site to join the conference, as shown in Figure 4-15.

Figure 4-15 A site that has been added




----End

Unmute Microphone

If the microphone of a site is unmuted by the chair site, the site can be heard by the other sites in the conference.

Step 1 Click **Unmute Microphone**.

Step 2 Choose a site whose microphone is in  state, and click the site name.


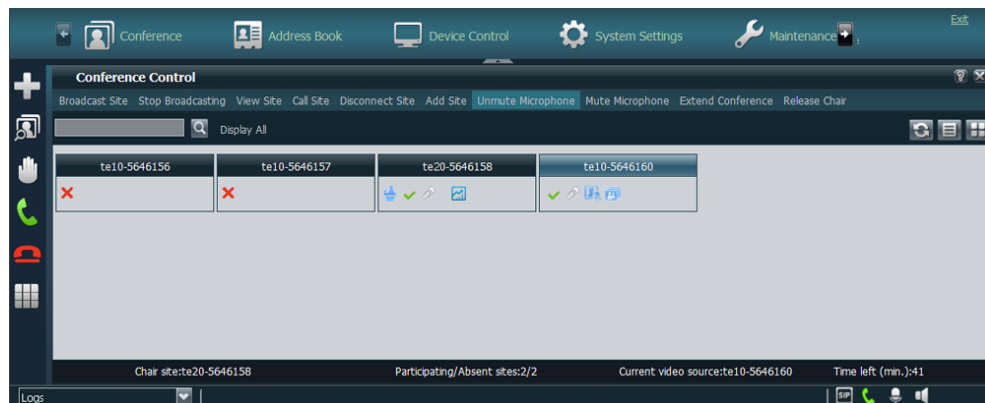
When the  icon is displayed, the microphone of the conference site has been unmuted, as shown in Figure 4-16.

Figure 4-16 Unmuting a microphone




----End

Mute Microphone

If the microphone of a site is muted by the chair site, the site cannot be heard by the other sites in the conference.

Step 1 Click **Mute Microphone**.

Step 2 Choose a site whose microphone is in  state.


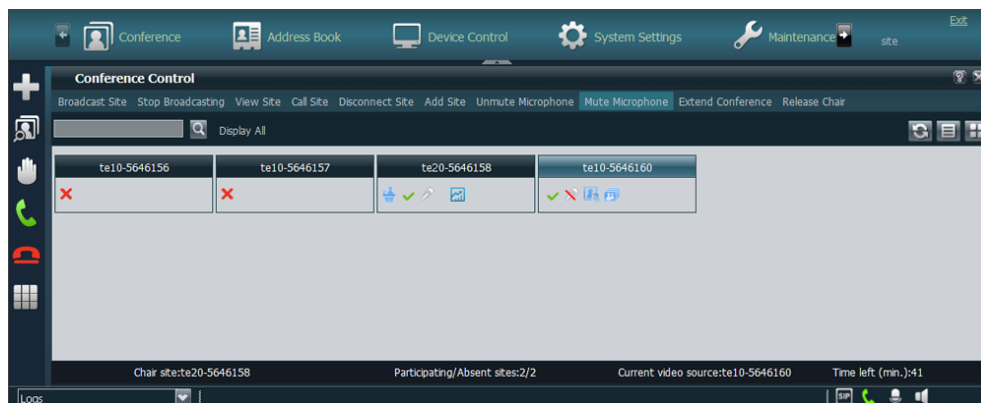
When the  icon is displayed, the microphone of the conference site has been muted, as shown in Figure 4-17.

Figure 4-17 Muting a microphone

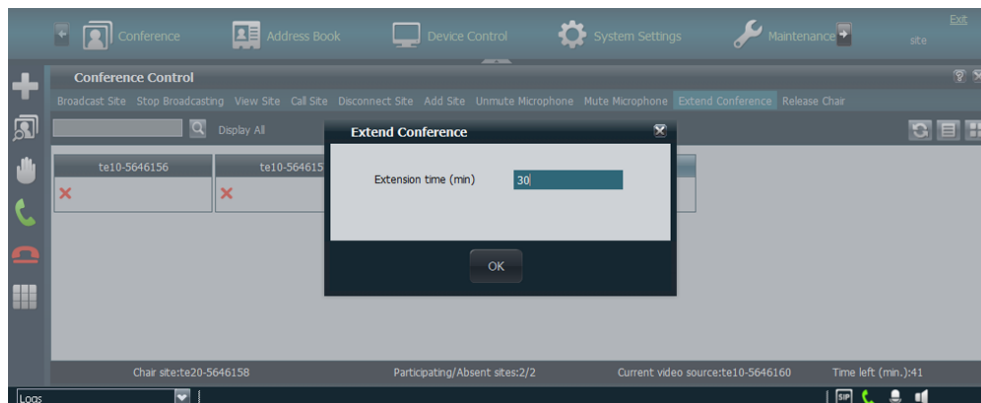
----End

Extend conference

If a conference is not likely to be complete by the scheduled time, the chair site can extend the conference using the **Extend Conference** function.

Extend the conference by 30 minutes at most at a time.

Step 1 Click **Extend Conference**, as shown in Figure 4-18.

Figure 4-18 Extending a conference

Step 2 Set the extended duration, click **OK**.

----End

Release Chair

The chair site uses this function to release chair control rights. Other sites can request chair control rights only after chair control rights are released.

Step 1 Click **Release Chair**.

Step 2 Click **OK** as prompted.

----End

4.4 Starting Presentation

To share the content on a computer, connect your computer to the endpoint. During presentation sharing, remote sites can watch the content shared on your computer screen.

Prerequisites

The presentation function is enabled, and the presentation parameters are set correctly. The endpoint has the presentation function enabled by default. The default presentation parameters are able to start presentation. If you want to set the presentation parameters based on your actual needs, see the *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.

The presentation source has been connected.

The AirPresence client is unavailable when you are using the remote desktop.

The AirPresence client can run on a Windows or Mac computer.

- The following 32- and 64-bit Windows operating systems are supported:
 - Windows XP
 - Windows Vista
 - Windows 7
 - Windows 8
 - Windows 10
- The following 32- and 64-bit Mac operating systems are supported:
 - OS X 10.7
 - OS X 10.8
 - OS X 10.9
 - OS X 10.10
 - OS X 10.11

Procedure

- Wired connection
Use a cable to connect the computer to a video input port on the endpoint.endpoint.

Step 1 Click **Conference > Share Presentation**. The **Share Presentation** dialog box is displayed.

Step 2 Click **Share**.


To stop presentation sharing, click **Stop**.

----End

- AirPresence Client Connection



Step 1 In the computer browser address box, enter the endpoint IP address and press **Enter**.

Step 2 On the login page, click **Download AirPresence Client** and install the client as prompted.

The  icon of the AirPresence client is displayed on the desktop when the installation is complete.

Step 3 On the computer desktop, double-click . The AirPresence dialog box is displayed.

Step 4 Connect the AirPresence client to your endpoint using either of the following methods:

- In the list of endpoint search results, select an endpoint to connect, and click .
- Enter the IP address of your endpoint and click .

Step 5 In the dialog box that is displayed, enter the AirPresence password (default: Change_Me), and click **Connect**.

 **NOTE**

When the **Received a connection request from an AirPresence client. Accept the request?** message is displayed on the endpoint web interface and remote control UI, select **Yes**. The client then successfully connects to the endpoint without any passwords.

If the endpoint is not used in a conference, the computer desktop is shared as a presentation with the endpoint.

If the endpoint is used in a conference, you can click **Share** to send the computer desktop to all sites.

----End

4.5 Setting the Answering Mode

On the endpoint web interface, you can set the answering mode.

Background

The following answering modes are available:

- **Manual** (default): Your endpoint prompts you to handle a call when the call comes in.
- **Auto**: Your endpoint automatically answers incoming calls when not being used in a conference.

Procedure

Step 1 Choose **System Settings > Conference** and click the **General Settings** tab.

Step 2 Set **Answer mode** to **Manual** or **Auto**.

----End

4.6 Muting the Local Microphone After Answering a Call

On the endpoint web interface, you can set the function of automatically muting the local microphone after the endpoint answers a conference invitation call.

Prerequisites

This parameter is available only after **Answer mode** is set to **Auto**. For details about how to set the answering mode, see 4.5 Setting the Answering Mode.

Background

If this function is enabled, the endpoint automatically mutes all the sound (such as microphone input) after being called to join a conference. Remote sites cannot hear the local sound.

Procedure

Step 1 Choose **System Settings > Conference** and click the **General Settings** tab.

Step 2 Set **Mute local audio for answered calls** to **Enable** or **Disable**.

----End

4.7 Using the Do-Not-Disturb Function

If you do not want to be disturbed by incoming calls, you can enable the Do-not-disturb function.

Step 1 On the endpoint web interface, choose **Conference > Do Not Disturb**.

The **Do Not Disturb** dialog box is displayed.

Step 2 Select **Enable** for **Do Not Disturb** and click **OK**.



NOTE

To disable the DND function, set **Do Not Disturb** to **Disable**, and click **OK**.

After an endpoint power-off, settings will not be saved, and will be restored to defaults.

----End

5 Device Control

5.1 Controlling Cameras

You can control the camera of an endpoint on its web interface or remote control UI.

5.1.1 Using the Remote Control

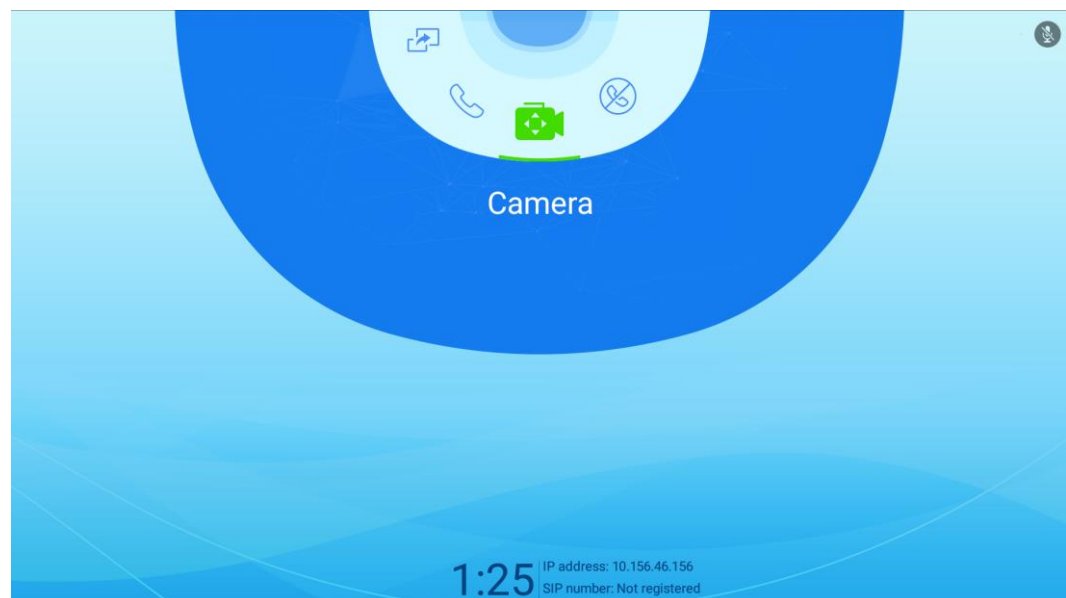
You can adjust local and remote cameras using the remote control.

Adjusting the Focal Length

You can use PTZ to zoom the local camera in or out.

Step 1 Choose **Camera** to access the **Camera** screen, as shown in Figure 5-1.

Figure 5-1 Camera screen




NOTE

If you have adjusted the focal length to its minimum value by pressing the volume down button, you cannot pan or tilt the camera using the arrow buttons.

Step 2 Press the side volume buttons to zoom in or out on video images shot by the camera.

 **NOTE**

Press  on the remote control to adjust the camera to its home position.

----End

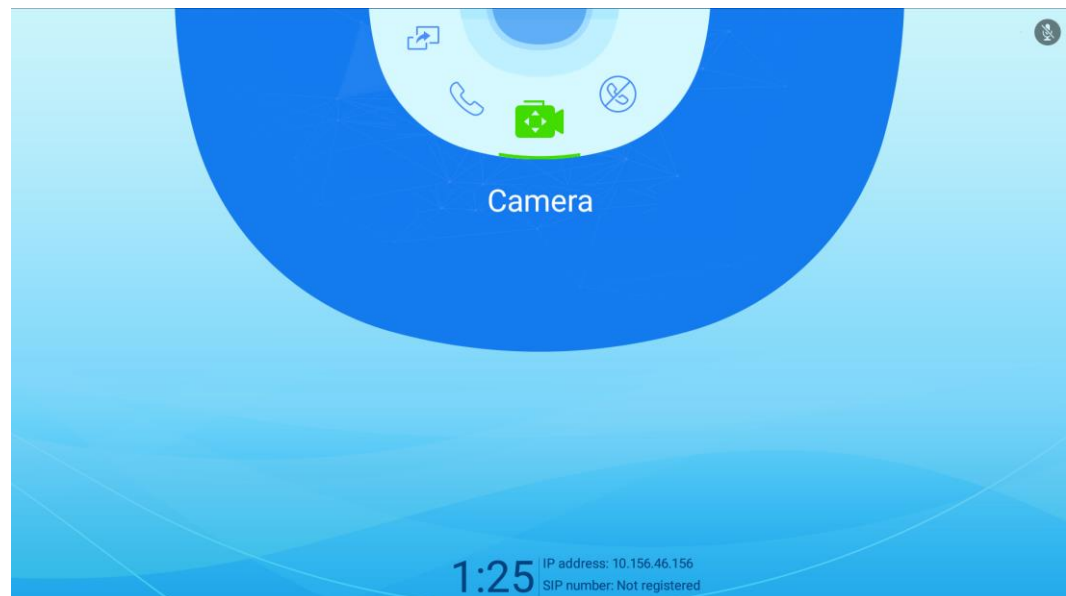
Controlling the PTZ

You can pan, tilt, and zoom the local camera.

Perform as follows:


Step 1 Choose **Camera** to access the **Camera** screen, as shown in Figure 5-2.

Figure 5-2 Camera screen



Step 2 Press the arrow buttons on the remote control to pan or tilt the camera.

 **NOTE**

Press  on the remote control to adjust the camera to its home position.








----End

5.1.2 Using the Web Interface

Using the web interface, you can pan, tilt, and zoom (PTZ) the local camera to view what you want.

Prerequisites

You are familiar with the following buttons for camera control:

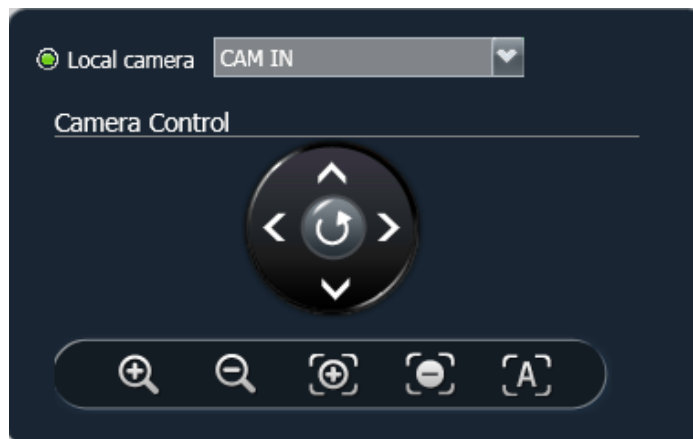
- : Turns the camera upward, downward, leftward, and rightward.
- : Turns the camera forward.
- : Enlarges the image taken by a camera.
- : Zooms in on a scene.
- : Shrinks the image taken by a camera.
- : Zooms out on a scene.
- : Automatically adjusts the camera focus.

Procedure

Step 1 Choose **Device Control > Device Control**.

Step 2 In the upper right corner of the **Video Control** page, select the camera you want to control, as shown in Figure 5-3.

Figure 5-3 Camera control



Step 3 Click the controls shown in Figure 5-3 to control cameras.

----End

5.2 Selecting Video Sources

On the endpoint web interface, you can select local video and presentation input sources and video output sources.

Prerequisites

The computer desktop to be displayed as presentation has a resolution and refresh rate supported by the endpoint. For details about how to set video output parameters, see the **Configuring Video Output** section in the *Web Online Help*.

Background

- Selecting video input sources
If more than one video source is connected to an endpoint, you can specify a main video source and an auxiliary one. A video source can be a computer, recorder, or DVD player.
- Selecting video output sources
In a conference, you can choose to deliver video or presentation of the local or remote site from the video output port.

Procedure

Step 1 Choose **Device Control > Device Control** and click **Video Control**.

Step 2 Select your desired video input and output sources.

----End

5.3 Setting Preferred Video Parameters

If you want to move the small pane in PiP video, enable the image offset function first. If video blurs or jitters, you need to adjust the sampling phase.

Background

Picture offset may occur in video input or output, such as when the computer desktop is displayed on the display device.

A blurring or slight jitter issue may occur in the video displayed on the display device. In this case, you can set the sampling phase to adjust the color.

Procedure

Step 1 Choose **Device Control > Device Control** and click the **Preferred Video** tab.

Step 2 Adjust the video parameters described in Table 5-1.

Table 5-1 Video parameters

| Parameter | Setting |
|------------------------------|---|
| Image Offset | Select Horizontal offset or Vertical offset and drag the slider to adjust the image offset on the video input and output ports. |
| Sampling Phase | Drag the slider to adjust the sampling phase for the PC IN port. |
| Small Window Position Offset | Drag the slider to adjust the offset for the Picture in Picture (PiP) window. |

| Parameter | Setting |
|-------------------|---|
| Output Adjustment | <p>Drag the slider to adjust the size of the output video. If your monitor specifications are low, and the video output from the endpoint does not display properly, set this parameter to fix the display issue.</p> <p>Before setting this parameter, make sure:</p> <ul style="list-style-type: none">• The endpoint is connected to the monitor using a standard cable.• The Extended Display Identification Data (EDID) from the monitor can be correctly read by the endpoint. |

----End

6 Address Book Management

On the web interface or remote control UI of the endpoint, you can perform operations on the address book, including adding sites and groups, querying and sorting sites, and importing or exporting the address book.

**NOTE**

The address book settings must be the same as those specified on the address book server; otherwise, the address book cannot be downloaded. You can operate the address book by following the instructions in the *TE20 Videoconferencing Endpoint V500R003C00 Configuration Guide*.

6.1 Adding Sites Using the Web Interface

On the endpoint web interface, you can add sites to the address book so that you can join conferences quickly and manage sites conveniently.

Procedure

Step 1 Choose **Address Book > Address Book**.

Step 2 Click **Add Site** and set the site parameters listed in Table 6-1.

Table 6-1 Site parameters

| Parameter | Description | Setting |
|-----------|---|--|
| Name | Specifies the name of the site. This site name is superimposed on the site video. | The value can contain a maximum of 64 characters, including digits, letters, and special characters. |
| Category | Specifies the conferencing scenario of the site. <ul style="list-style-type: none">• Ordinary site: Select this option for a traditional videoconferencing site.• Telepresence site: Select this option for a Huawei three-screen telepresence site.• CT site: Select this option for a Cisco TelePresence site. | The default value is Ordinary site . |

| Parameter | Description | Setting |
|---------------------|--|--|
| Type | Specifies the type of the line the site uses to access the videoconferencing network. <ul style="list-style-type: none"> If you select IP, your endpoint will use the protocol set for Preferred IP protocol to call the site. If you set Category to CT site, the available value for Type is SIP. | The default value is H.323 . |
| Rate | Specifies the data transmission rate of the line selected for the remote endpoint. The supported data transmission rates vary depending on the type of the site you want to call. | Select the highest available data transmission rate. |
| Country/Region code | Specifies the country or area where the site is located. This parameter is available only for integrated services digital network (ISDN) and public switched telephone network (PSTN) sites. | No default value is set for this parameter. |
| Area code | Specifies the area code for the site. This parameter is available only for ISDN and PSTN sites. | No default value is set for this parameter. |
| Number | Specifies the site number used to place calls between sites. This parameter is unavailable for an ISDN site. <ul style="list-style-type: none"> IP, E1, 4E1, ISDN, and H.323 phone site numbers are allocated by the videoconferencing service provider. PSTN site numbers are telephone numbers. | No default value is set for this parameter. |
| IP address | Specifies the IP address of the site. NOTE <ul style="list-style-type: none"> The IP address parameter is unavailable for a Ordinary site whose Type is ISDN, PSTN, E1, or 4E1. The IP address parameter is unavailable for a Telepresence site. This parameter is unavailable if you set Category to CT site. | No default value is set for this parameter. |
| URI | Specifies the uniform resource identifier (URI) of the site, for example, abcd@huawei.com . NOTE This parameter is available only when Type is set to IP , H.323 , or SIP . | No default value is set for this parameter. |
| Center codec number | These parameters are available only after Category is set to Telepresence site . | No default values are set for these parameters. |
| Center codec | These parameters specify the numbers and IP | |

| Parameter | Description | Setting |
|--|---|---|
| IP address Left codec number Left codec IP address Right codec number Right codec IP address | addresses of the center, left, and right codec participants. Numbers are assigned to participants by a specific videoconferencing service vendor and used by them to set up calls. NOTE The Center codec IP address, Left codec IP address, and Right codec IP address parameters are unavailable for a Telepresence site whose Type is E1 or 4E1. | |
| Screen type | This parameter is available only after Category is set to CT site . Set this parameter to Uni-screen or Tri-screen . | The default value is Tri-screen . |
| Line 1 #1 Line 1 #2 Line 2 #1 Line 2 #2 Line 3 #1 Line 3 #2 | Specify the numbers your endpoint uses to call the site. These parameters are available only for ISDN sites. <ul style="list-style-type: none"> If the ISDN site rate is set to a value ranging from 64 kbit/s to 2048 kbit/s, set Line 1 #1 only, because you only need to dial that number to call the site. If the ISDN site rate is set to 2, 3, 4, 5, or 6 x 64 kbit/s, set the other required parameters as well, because you need to dial the BRI line numbers one by one to call the site. For example, when the ISDN site rate is set to 2 x 64 kbit/s, set the first two parameters Line 1 #1 and Line 1 #2; when the ISDN site rate is set to 3 x 64 kbit/s, set the first three parameters Line 1 #1, Line 1 #2, and Line 2 #1, and so forth. Line 1 #2 specifies the second number of the first BRI line. | No default value is set for this parameter. |
| Sort ID | Specifies the sequence number of the site in the address book. | The default value is 0 . |

Step 3 Click **Save**.

The settings take effect immediately. The new site is listed in the address book.

----**End**


6.2 Adding Groups Using the Web Interface

If certain sites regularly join the same conference, you can define these sites as a group on the endpoint web interface.

Procedure


Step 1 Choose **Address Book > Address Book**.

Step 2 Click **Add Group**. In **Name**, enter the group name.

Step 3 Select one or more sites and click .

The selected sites are displayed under **Group Members**.

 **NOTE**

To delete a site listed in **Group Members**, select the site and click , To delete all sites, click



Step 4 Click **Save**.

The new group is listed in the address book.

----End

6.3 Modifying or Deleting Sites or Groups in the Address Book Using the Web Interface

On the endpoint web interface, you can manage address book records, such as searching for, modifying, deleting, and sorting them.

Searching for Records

Enter keywords in the search box and click  to search the local address book for local sites and groups or search the LDAP server for LDAP sites.

- Select one from the found local or LDAP sites and click **Call** to call the site.
- Select one from the found LDAP sites and click **Save** to save the site to the local address book.

Editing Records

Click the name of a site or group in the address book. On the displayed editing page, modify the settings for the site or group.

Deleting Records

Select the site or group you want to delete and click **Delete**.

Sorting Records

If there are multiple sites on the address book page, conference-related pages, or other pages, you can sort the sites based on their properties, such as by name, number, line type, online status, and type.

From the site lists on some of these pages, you can click one of five letter ranges, **A-E F-J K-O P-T U-Z**, to display the sites whose names start with letters within that range.

6.4 Importing and Exporting Address Book

From the endpoint web interface, you can export the local address book to the local computer or a server. You can also import the modified address book to the endpoint, after which the records in the address book are displayed on the address book page.

Background

The exported address book is saved to a file in vCard format. The file name extension is .vcf.

When exporting the address book, you can specify the character encoding format to either of the following:

- China: The character set is GB2312.
- Other countries: The character set is UTF-8.

For example, you can export records from the address book of endpoint A, modify the records, and then import these records to the address book of endpoint B. The exported contacts file may contain personal information. Keep the file in a safe location to prevent personal information disclosure.

Procedure

Step 1 Choose **Address Book > Address Book**.

Step 2 Perform either of the following:

- To import new entries to the local address book, click **Import to Local Address Book**.
- To export the local address book, click **Export from Local Address Book**.

----**End**

7 System File Management

On the endpoint web interface, you can manage system configurations or files, such as importing or exporting configurations and backing up configurations simply by one click.

7.1 Importing and Exporting Settings

You can import or export settings on the endpoint web interface. After your endpoint is restored to its default settings, you can import previously exported settings.

Background

After your endpoint is restored to its default settings upon a fault, you can import previously exported settings.

For example, when your endpoint is faulty and needs to be restored to its default settings, export the existing settings before the restoration. After you restore your endpoint, directly import the exported settings instead of manually setting the parameters. This saves your time.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import/Export Settings**.

The **Import/Export Settings** page is displayed.

Step 3 Perform either of the following:

- To import system settings, click **Import Settings**.
- To export system settings, click **Export Settings**.

The web administrator password is required when you import the configuration file. After the configuration file is imported successfully, the endpoint automatically restarts for the configuration file to take effect.

----End

7.2 Backing Up Settings

The administrator can use the **One-Click Backup** function to create a configuration backup file for your endpoint. If some parameter settings under **System Settings** are inadvertently deleted or changed, you can use this backup file to restore all settings under **System Settings** to the pre-backup settings.

Background

If a configuration backup file is already stored on your endpoint, a new configuration backup file will replace the original one.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **One-Click Backup**.

Step 3 On the **One-Click Backup** page, click **Back Up Settings**.

Your endpoint then starts to create a configuration backup file. When the backup is complete, a notification message is displayed.

----End

Follow-up Procedure

To restore all settings under **System Settings** to the pre-backup settings, click **Restore Backup Settings**. Your endpoint will then restart and restore the settings.

7.3 Creating and Downloading a CSR File

You can create and export a Certificate Signing Request (CSR) file from the endpoint web interface.

Prerequisites

The local private key password file has been imported.

Background

You can send the CSR file to a certification organization to generate an authentication certificate for your endpoint.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Export CSR File**.

Step 3 Enter the information about the CSR file, as shown in Table 7-1. Then click **OK**.

Table 7-1 CSR file parameters

| Parameter | Description | Setting |
|--------------------------|--|---|
| Common Name (CN) | Specifies the name of the CSR file. | No default value is set for this parameter. |
| Organizational Unit (OU) | Specifies the organizational unit to which the CSR file belongs. | No default value is set for this parameter. |
| Organization (O) | Specifies the organization to which the CSR file belongs. | No default value is set for this parameter. |
| City or Locality (L) | Specifies the city or region to which the CSR file belongs. | No default value is set for this parameter. Example: New York |
| State or Province (ST) | Specifies the state or province to which the CSR file belongs. | No default value is set for this parameter. Example: State of New York |
| Country (C) | Specifies the country to which the CSR file belongs. | No default value is set for this parameter. Example: United States |

The created CSR file will be stored on the endpoint.

Step 4 Click **Download CSR file** to save the CSR file to the local computer.

----End

8 Operation UI Customization

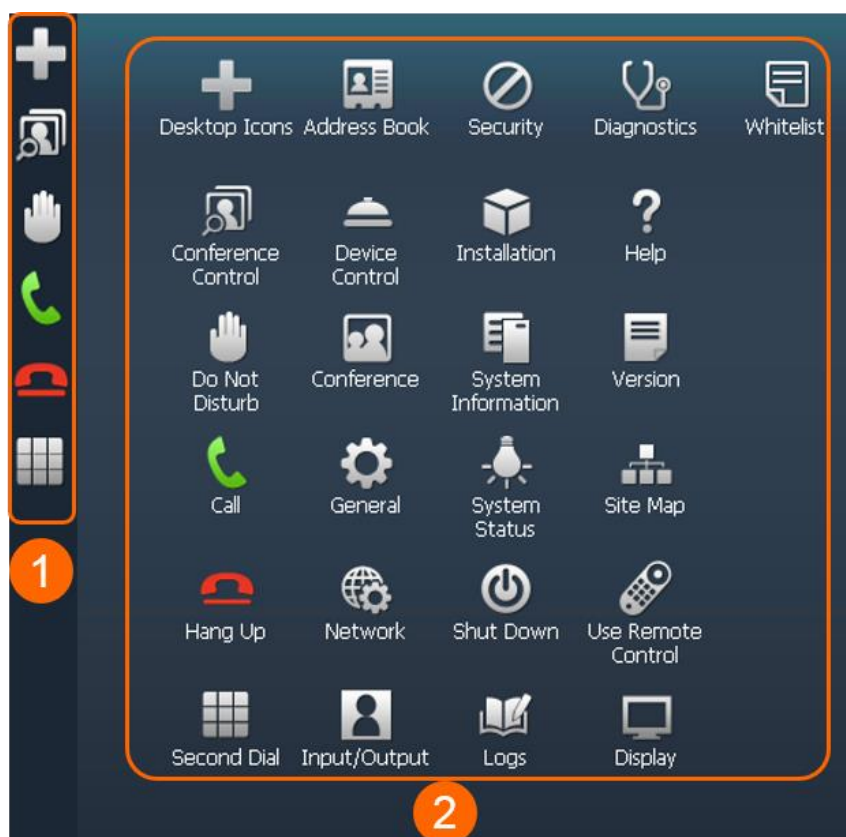
You can customize the web interface, remotely controlled UI, and touch panel UI for your special conference control requirements.

8.1 Customizing the Web Interface

On the endpoint web interface, you can customize the shortcut bar and desktop icons to be displayed on the web interface.

Figure 8-1 shows the shortcut bar and desktop icons.

Figure 8-1 Shortcut bar and desktop icons



- (1) Shortcut bar
- (2) Desktop icons

8.1.1 Desktop Icons

You can customize icons to be displayed on the home page of the endpoint web interface.

Procedure

- Step 1** Choose **System Settings** > **Display** and click the **User defined** tab.
- Step 2** Click **Desktop Icons** and select the icons you want to display on the desktop.
- Step 3** Follow the onscreen instructions to complete your settings.

----End

8.1.2 Shortcut Bar Icons

You can customize icons (a maximum of 10) to be displayed on the shortcut bar of the endpoint web interface.

Procedure

Step 1 Choose **System Settings > Display** and click the **User defined** tab.

Step 2 Click **Shortcut Bar Icons** and select the icons you want to display in the shortcut bar.

Step 3 Follow the onscreen instructions to complete your settings.



NOTE

To restore shortcut icons to the initial style, click **Restore Initial Style**.

----End

8.2 Customizing the Remote Control UI

You can customize which status icons are displayed on the home screen, helping you quickly understand the endpoint's status.

For details about common status icons, see [A Icons on the Remotely Controlled UI](#).

Choose **System Settings > Display**, click the **Icon** tab, and customize status icons.



Packet Loss Rate Icon

By comparing the packet loss rate on the current network with threshold A and threshold B, the endpoint determines whether to display the packet loss rate icon on the remotely controlled UI. The policy is as follows:



NOTE

Threshold A must be less than threshold B. Their value ranges are 0.1% to 100%. The default values for threshold A and threshold B are 1% and 5%, respectively.

- If the packet loss rate is less than or equal to threshold A, no packet loss rate icon is displayed.
- If the packet loss rate is between threshold A and threshold B,  is displayed.
- If the packet loss rate is greater than or equal to threshold B,  is displayed.

When **Serious packet loss notice** is enabled, the remotely controlled UI displays a text alert if the packet loss rate is greater than threshold B for 5 seconds or more.

Other Icons

A status icon is displayed on screens if the following conditions are met:

- The status icon to be displayed on screens is selected.
- The function or the condition that corresponds to the status icon has been enabled.

9 Routine Maintenance

Perform routine maintenance on the endpoint to know its running status and detect its exceptions in time.

9.1 Maintenance Items

Table 9-1 describes the maintenance items, tasks, and periods of the endpoint.

Table 9-1 Maintenance items, tasks, and periods

| Maintenance Item | Maintenance Task | Maintenance Period |
|-----------------------|---|---------------------------------|
| Device indicators | Check whether the device is working properly. | Daily |
| Operating environment | Check whether the operating temperature is within the required range. | Weekly |
| | Check the relative humidity (RH). | Weekly |
| Device cleanliness | Clean the device. | Weekly |
| Device connection | Check whether the device is connected properly. | Weekly |
| Device alarms | Check and clear device alarms. | Daily |
| System status | Check whether the system status is normal. | Daily |
| Backup | Back up configuration data regularly. | Monthly |
| Resume | Restore configuration data. | Perform this task if necessary. |
| Restore Default | Restore the endpoint to factory defaults when a | Perform this task if necessary. |

| Maintenance Item | Maintenance Task | Maintenance Period |
|------------------|----------------------------|--------------------|
| | critical exception occurs. | |

9.2 Checking the Indicator Status

To ensure that your endpoint runs properly, check its indicator status regularly.

Background

By checking the status of indicators on the endpoint's front panel, you can know the endpoint's running status, for example, working properly, sleeping, and working at a high temperature. If any indicator does not perform as expected, tackle the problem in time to ensure proper running of the endpoint.

Checking Indicators on the endpoint

Check the status of indicators on the endpoint by following the instructions described in Table 9-2 and perform maintenance tasks accordingly.

Table 9-2 TE20 Indicator status

| When The Indicator Is... | The TE20 Is... |
|--|---|
| Off | Powered off. |
| Blinking green twice per second | Powering on. |
| Blinking green four times per second | Being upgraded. |
| Steady green | Working properly. |
| Blinking green (on for 1s, off for 2s) | Standby. |
| Blinking once | Responding to the press on a button on the remote control. |
| Blinking once per second | Responding to the press and hold on a button on the remote control. |
| Steady red | Having a hardware fault. |
| Steady orange | Having a software fault. |
| Blinking orange twice per second | Overheated. |

9.3 Checking the Operating Environment

To ensure that your endpoint runs properly, check its operating environment regularly.

Table 9-3 describes the items you need to check to ensure a sound operating environment.



NOTICE

If any of the items goes beyond the specified range, power off the endpoint, improve the item to meet the requirement, and restart the endpoint.

Table 9-3 Operating environment

| Item | Requirement |
|-----------------------|---|
| Operating temperature | <ul style="list-style-type: none">Working status: 0 °C to 40 °C (32 °F to 104 °F)Non-working status: -40 °C to +70 °C (-40 °F to 158 °F) |
| RH | <ul style="list-style-type: none">Working status: 10% to 80%Non-working status: 0% to 95% |

9.4 Checking the Cleanliness

To ensure that your endpoint runs properly, check its cleanliness regularly.

Background

If the endpoint runs for a long period of time but is not cleaned, its body, ports, heating vents, and camera lens may be covered with dust. Its performance may be compromised, impacting user experience. Therefore, it is necessary to regularly clean the endpoint and its peripherals, helping extend their lifecycle and improve user experience.

Checking the Endpoint Cleanliness

Check the cleanliness of your endpoint regularly to ensure that it runs properly in a long term and delivers superb conference experience.

Table 9-4 describes the items to be checked. If any of them does not meet the requirement, clean it accordingly.

Table 9-4 Cleanliness items

| Item | Requirement |
|-------------------------|--|
| Embedded camera lens | The camera lens is clean. |
| Ports and heating vents | The ports and heating vents are clean. |
| Device body | The device body is clean. |

9.5 Checking the Connection Status

To ensure that your endpoint runs properly, check its connection status regularly.

Background

The endpoint's cables may be loose or disconnected during its operation. The administrator needs to regularly check the connection status of the endpoint to ensure that it can connect to video conferences as expected.

Items to Check

- Regularly check whether the cables connecting the endpoint to the peripherals and power supply are securely connected. It is recommended that you perform this task once a week. If any of the cables is loose, reconnect the cables securely.
- Power on the endpoint and check whether its communication cables are connected securely. It is recommended that you perform this task once a week.
- Use the endpoint to call some other endpoints in different communication modes, such as calling over a broadband network. If a call cannot be set up, check whether the cables are connected securely and whether the communication parameters are set correctly. If the problem persists, contact the videoconferencing network administrator to check the network.

9.6 Checking Alarms

To ensure that your endpoint runs properly, check its alarms regularly.

Background

Periodically check whether the endpoint has alarms. If it has alarms, follow the instructions described in the *Alarm Handling* to clear them, ensuring that the endpoint runs properly.

Procedure

To check alarms on the endpoint, perform the following steps:

- Step 1** Log in to the endpoint web interface as the administrator.
- Step 2** Check whether there are alarm notification messages on the web interface.
- Step 3** Find the handling suggestions for alarms in the *Alarm Handling* by alarm ID and clear the alarms accordingly.

----End

9.7 Checking the System Status

To ensure that your endpoint runs properly, check its system status regularly.

Background

- Line status information includes: IPv4, IPv6, network port model, WLAN IP address, Whether to use GK and H.323 site numbers, Whether to use SIP site numbers, running time, and cloud platform activation and subscription status.
- Input port status information includes: built-in camera, PC IN port, USB port, and wireless connection status of presentation streams.

Checking the Line Status

To check the line status, perform the following steps:

Step 1 Log in to the endpoint web interface as the administrator.

Step 2 Choose **Maintenance > System Status**.

The **System Status** page is displayed.

Step 3 Click the **Line Status** tab.

Check line status information.

Step 4 If any exception is found, tackle it in time.

----End

Checking the Input Port Status

To check the input port status, perform the following steps:

Step 1 Log in to the endpoint web interface as the administrator.

Step 2 Choose **Maintenance > System Status**.

The **System Status** page is displayed.

Step 3 Click the **Input Interface Status** tab.

Check input port status information.

Step 4 If any exception is found, tackle it in time.

----End

9.8 Checking the System Information

To ensure that your endpoint runs properly, check its system information regularly.

Background

Regularly check the system information of the endpoint to know its conference resources and capabilities, facilitating appropriate allocation of conference resources.

Procedure

Step 1 Log in to the endpoint web interface as the administrator.

Step 2 Choose **Maintenance > System Information**.

The **System Information** page is displayed.

Step 3 Table 9-5 describes the items to be checked.**Table 9-5** Items to check

| Item | Task |
|---------------------------------|--|
| Audio | The audio codec capability works properly. |
| Video | The video codec capability works properly. |
| Interface/Bandwidth | <ul style="list-style-type: none">• Check network interfaces supported by the endpoint.• Check the maximum network bandwidth supported by each interface. |
| SIP | Check whether the device supports SIP-based communication. |
| Dual stream | Check whether the device supports dual-stream calls. |
| H.235 Encryption | Check whether the device supports H.235 encryption. |
| Wi-Fi | Check whether the device supports Wi-Fi access. |
| Maximum presentation resolution | Check the maximum presentation resolution of the device. |
| Maximum encoding capacity | Check the maximum encoding capability of the device. |
| Maximum decoding capacity | Check the maximum decoding capability of the device. |
| MAC address | Check the MAC address of the device. |
| Electronic label | Check the unique identifier of the device. |
| Zoom level | Check the zoom level of the device. |

----End

9.9 Backup and Restoration

Regularly back up the system configuration file of the endpoint and use the backup file to restore the system after an exception occurs.

Background

- You can use the **One-Click Backup** function to create a backup file for the endpoint.
- If a configuration backup file is already stored on your endpoint, the new backup configuration file will overwrite the original one.

- After the restoration is complete, the endpoint will automatically restart. The settings under **System Settings** will be restored to those contained in the backup configuration file.
- Before upgrading the endpoint, it is recommended that you back up the settings under **System Settings**. If the upgrade fails, you can use the backup data to restore the system.
- If some parameter settings under **System Settings** are inadvertently deleted or modified, you can use this backup file to restore all the settings.

Backup Settings

The Backup Settings procedure is as follows:

Step 1 Log in to the endpoint web interface as the administrator.

Step 2 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 3 Click **One-Click Backup**.

The **One-Click Backup** dialog box is displayed.

Step 4 Click **Backup Settings**.

The endpoint starts backing up its configuration file. If the backup is complete, a success message will be displayed.

----End

Using the Backup Configuration File to Restore the System

The restoration procedure is as follows:

Step 1 Log in to the endpoint web interface as the administrator.

Step 2 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 3 Click **One-Click Backup**.

The **One-Click Backup** dialog box is displayed.

Step 4 Click **Restore Backup Settings**.

The endpoint starts using the backup configuration file to restore the system.



NOTE

After the restoration is complete, the endpoint will automatically restart.

----End

9.10 Restoring Factory Settings

Use the **Restore Default** function to restore the endpoint to its factory settings.

Prerequisites

You have obtained the ESN of the endpoint that is to be restored to factory settings.

Log in to the endpoint web interface and choose **Help > Version**. On the version information page, you will see the ESN of the endpoint.

Background

- Before restoring the endpoint to its factory settings, back up its configuration file.
- After the endpoint is restored to its factory settings, some of its information will be lost, including site information in the address book, call records, and logs.

Procedure

Step 1 Log in to the endpoint web interface as the administrator.

Step 2 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 3 Click **Restore Default**.

Step 4 Enter the ESN of the endpoint.

Step 5 Click **Restore Default**. In the confirm dialog box, click **Confirm**.

----End

10 Security Maintenance

To ensure proper and secure running of the telepresence system, you need to know application layer accounts and their default passwords and security maintenance methods, as well as security maintenance principles and policies at the system, network, and management layers.

10.1 Overview

This section describes the overall purpose of security maintenance, as well as specific purposes of security maintenance at the application layer, system layer, network layer, and management layer.

10.1.1 Purpose of Security Maintenance

Security management regulations should be established based on security maintenance suggestions and problems found in daily operations to ensure proper and secure running of the videoconferencing system.

Now application systems face severe security threats. Once problems occur, business might be disturbed, profits reduced, or even systems break down. Users must build up and maintain the application system security from different layers, and discover and solve potential threats in advance.

Besides, considering the endless emergence of safety threats, a mere dependence on technology can hardly ensure the application system security. Users must build up a safety management system based on security maintenance suggestions and problems they found during the use of the endpoint to ensure a smooth and safe operation of the endpoint.

10.1.2 What Is Layered Security Maintenance

Service systems must be maintained at the application layer, system layer, network layer, and management layer.

According to the target and purpose of security maintenance, maintenance personnel must safeguard the service system from different layers.

Application Layer

Security maintenance of the application layer is to protect the endpoint and its web management system so that they can provide services to users with a smooth operation.

System Layer

Security maintenance of the system layer is to ensure a smooth operation of the operating system, which can support the operation of application software.

Network Layer

Security maintenance of the network layer is to ensure that network devices, such as the switch, router, and firewall, function properly and that security strategies are implemented at the network layer.

Management Layer

Security maintenance of the management layer is to strengthen people's management and avoid threats. Maintenance from the management layer involves the maintenance operations at all preceding layers.

10.2 Application Layer Security

This section describes application layer accounts and their default passwords and functions, as well as security configurations at the application layer.

10.2.1 Application Layer Account List

This section describes application layer accounts and their default passwords, functions, and configuration methods. To ensure account security, you are advised to change the password at the first login and regularly change the password afterward.

Administrator Password of the Remotely Controlled UI

This section describes the default password of the remotely controlled UI administrator and relevant settings and precautions.

The default administrator password of remote control interface is **12345678**. To improve device security, set a password at your first login and regularly change the password afterward.

NOTE

It is recommended that you set a complex password. A simple or empty password brings security risks.

To set the administrator password for logging in to the remote control interface, perform the following steps:

- On the remotely controlled UI, choose **System Settings > More > Administrator Password**, and set the password.
- On the web interface, choose **System Settings > Security > GUI**, and set the password.

You need the administrator password to access the **System Settings** page. Contact the system administrator to obtain the password.

Web Management Account

Web login accounts are classified into **admin**, and **api**. Keep your administrator account and password secure to prevent personal information disclosure.

The similarities of **admin**, and **api** accounts are as follows:

- The account and password can be used to log in to the web interface, Telnet, and SSH.
- Rights except user name and password change policies are the same: able to read and write other configuration items; and able to invoke all HTTP interfaces.

The differences of **admin**, and **api** accounts lie in the rights in changing other user names and passwords:

- The **admin** account can be used to change the user name and password of the **api** account with the verification of the old password of the **admin** account.
- The **api** account can be used to change the user name and password of the **admin** account with the verification of the old password of the **api** account.

Table 10-1 lists the default user names and passwords for **admin**, and **api** accounts.

Table 10-1 admin and api accounts

| Account Name | Default Password | Function | Remarks |
|--------------|------------------|------------------------|---|
| admin | Change_Me | Administrator account. | To ensure account security, you are advised to change the password at the first login and regularly change the password afterward. On the web interface, choose System Settings > General > Personal , and change the user name and password. |
| api | Change_Me | API account. | |

System Connection Whitelist

The whitelist helps enhance videoconferencing security. After you configure a whitelist, only devices with the IP addresses specified in the whitelist can connect to the endpoint.



NOTICE

Set the whitelist under the guidance of technical support engineers.

The endpoint whitelist is empty by default. That is, all IP addresses are allowed to connect to the endpoint. If the endpoint is deployed on a public network, it is recommended that you add frequently-used IP addresses or IP address segments to the whitelist. This approach helps defend against potential network threats, such as flood attack and slow HTTP attack. You must add the IP addresses of the following devices to the whitelist:

- PC that is used to access the endpoint web interface
- Videoconferencing MCU
- SMC2.0
- Recording server

To set the whitelist on the web interface, perform the following steps:

1. Choose **System Settings > Whitelist**.
2. Select **Enable**.

If **Enable** is deselected, the whitelist is invalid. That is, all IP addresses are allowed to connect to the endpoint. You can modify the whitelist only after selecting **Enable** here.

3. Click **Add** and set **IP address** and **Mask length**.
4. Click **OK**. The settings take effect immediately.



NOTE

If the endpoint is attacked and its web interface stops working, you can log in to the endpoint using the serial port, enter the shell, and execute the **iptables** command to set the whitelist.

TR-069 Connection Credential and Account

The TR-069 server is connected to centrally manage endpoints.

To centrally manage endpoints on the TR-069 server, log in to the web interface, choose **System SettingsNetworkTR069**, and set the TR-069 parameters listed in Table 10-2.

Table 10-2 TR-069 parameters

| Parameter | Description | Setting |
|-----------------------|--|---|
| TR069 | Specifies whether to enable the TR-069 function. If this function is enabled, the endpoint will send a session setup request to the Auto-Configuration Server (ACS). Start the ACS before enabling the TR-069 function. NOTE If you set this parameter to Enable , you must also set ACS User Name , ACS Password , ACS Server IP Address , Report Interval(s) , CPE User Name , CPE Password , and Authentication mode . | The default value is Disable . |
| ACS User Name | Specifies the user name authenticated by the ACS after receiving a session setup request from the endpoint. The user name has been specified on the ACS. | No default value is set for this parameter. |
| ACS Password | Specifies the password authenticated by the ACS after receiving a session setup request from the endpoint. The password has been specified on the ACS. | No default value is set for this parameter. |
| ACS Server IP Address | Specifies the ACS URL, which can be based on an IP address or domain name. <ul style="list-style-type: none"> • IP address-based URL example: http://10.10.10.1:8086 • Domain name-based URL example: http://company.acs.com:8086 (8086 indicates the ACS port number) | No default value is set for this parameter. |
| Report Interval(s) | Specifies the interval at which the endpoint | The default value is |

| Parameter | Description | Setting |
|---------------------|--|---|
| | sends a session setup request to the ACS. | 1800. It is recommended that this interval be shorter than the timeout period of the ACS. If this interval is longer than the timeout period, the ACS may be disconnected or the session status may not be updated in time after a session setup timeout. |
| CPE User Name | Specifies the user name authenticated by the endpoint after receiving a session setup request from the ACS. The user name has been specified on the ACS. | The default value is admin . |
| CPE Password | Specifies the password authenticated by the endpoint after receiving a session setup request from the ACS. The password has been specified on the ACS. | The default value is Change_Me . In addition, it must include at least two of the following: uppercase letters, lowercase letters, digits, and special characters. |
| Authentication mode | Specifies the mode in which the endpoint will be authenticated when accessing to the network management system. | The default value is Digest . If you set this parameter to None or Basic , the system will prompt you that the authentication mode poses security risks. To ensure security, set this parameter to Digest . The default value is recommended. |
| STUN | Specifies whether to enable the Simple Traversal of UDP through NAT (STUN) function. If this function is enabled, the endpoint can perform private-to-public network traversal using the STUN server on the TR-069 network. NOTE If you set this parameter to Enable , you must also set STUN Server IP Address , STUN Server Port , STUN listen port , STUN User Name , STUN Password , and STUN keep-alive period(s) . | The default value is Disable . |
| STUN Server IP | Specifies the IP address of the STUN | No default value is set |

| Parameter | Description | Setting |
|---------------------------------|--|--|
| Address | server. | for this parameter. Obtain the value of this parameter from the STUN server administrator. |
| STUN Server Port | Specifies the port number used by the STUN server to provide the private and public network traversal service. | The default value is 3478 . Obtain the value of this parameter from the STUN server administrator. |
| STUN listen port | Specifies the port provided by the endpoint for private and public service interaction with the STUN server. | The default value is 3000 . |
| STUN User Name STUN Password | Specifies the authentication user name and password of the STUN server. | No default value is set for this parameter. Obtain the value of this parameter from the STUN server administrator. It is recommended that the password contain at least 16 characters that consist of letters, digits, and special characters. |
| STUN keep-alive period(s) | Specifies the interval at which the endpoint sends a session setup request to the STUN server. | The default value is 150 . |

SSH and Telnet Login

The endpoint supports the Telnet login and Security Shell (SSH) login. Telnet is an insecure protocol. SSH is a cyber security protocol for remote access using the encryption and authentication mechanism in an insecure cyber environment. During SSH login, all user data are encrypted. To ensure the security, you are advised to use the SSH login.

- You can log in to the endpoint through port 23 using Telnet. **Telnet login** is set to **Do not allow** by default.

Telnet is an insecure communication protocol. You are advised to disable it. If you want to log in using Telnet, see section 10.2.6 SSH Access Control.

- You can log in to the endpoint through port 22 using SSH. **SSH** is set to **Do not allow** by default. If you want to log in using SSH, see section 10.2.6 SSH Access Control.

SSH/Telnet login accounts are the same as web login accounts. For details, see 10.2.1 Application Layer Account List.

Upgrade Password

The upgrade password is required when you use the upgrade tool to upgrade the endpoint.

By default, the upgrade password is **Change_Me**.

You are advised to change the password at the first login and regularly change the password afterward. On the web interface, choose **System Settings > Security > Upgrade password**, and change the password.



NOTE

If the default upgrade password is used, a confirm dialog box will be displayed after you choose to upgrade your endpoint on its remote control UI or web interface. The upgrade will start only after you confirm it.

AirPresence Password

The AirPresence password is used by an AirPresence client to connect to the endpoint. Users can download the AirPresence client from the endpoint web interface. After the AirPresence client successfully connects to the endpoint, users can connect the endpoint to presentation sources and share presentations without the use of any physical ports.

The default AirPresence password is **Change_Me**.

You are advised to change the password at the first login and regularly change the password afterward. The path for changing the password on the web interface is: **System Settings > Security > AirPresence**



NOTE

After being connected to the endpoint, the AirPresence client has the same rights as the **api** account. Keep the password secure.

AirPresence Whitelist

To enhance connection security, configure the AirPresence whitelist.



NOTE

Before configuring the Wi-Fi hotspot whitelist, ensure that **Connection over Wi-Fi only** have been enabled.

Configure the AirPresence whitelist as follows:

1. Choose **System Settings > Security > AirPresence**.
2. Click **Whitelist**.
3. Select **Enable**.
You can modify the whitelist only after selecting **Enable** here.
4. Click **Add** and set **IP address** and **Mask length**.
5. Click **OK**. The settings take effect immediately.

Information Required for Connecting to the Videoconferencing Network Management System

The endpoint communicates with and is remotely managed by the videoconferencing network management system using SNMP.

The videoconferencing network management system implements the following:

- Sets endpoint parameters, such as H.323 and SIP.
- Checks endpoint alarms.
- Backs up and restores endpoint settings.
- Upgrades the endpoint online.

To remotely manage the endpoint from the videoconferencing network management system, log in to the web interface of the endpoint, choose **System Settings > Network > SNMP Settings**, and set SNMP parameters, as shown in Table 10-3.

**NOTE**

To secure your account, it is recommended that you change the password upon the first login and regularly change the password afterwards. The password you set on the endpoint must be the same as that set in the videoconferencing network management system.

Table 10-3 Information required for connecting to the videoconferencing network management system

| Parameter | | Default Setting | Description | Remarks |
|-----------------|-----------------------|---------------------------|--|---|
| Common Settings | Enable SNMP | Enable | Indicates whether to enable SNMP. | When the endpoint is used as a client, the parameter settings must be the same as those in the videoconferencing network management system. |
| | Trap server address 1 | - | Indicates the videoconferencing network management server address used by the endpoint to report alarms. | |
| | Trap server address 2 | - | | |
| | Trap server address 3 | - | | |
| | Trap server port 1 | 162 | Indicates the videoconferencing network management server port number used by the endpoint to report alarms. | |
| | Trap server port 2 | 162 | | |
| | Trap server port 3 | 162 | | |
| | Trap version | v3 trap | Indicates the SNMP server version. | |
| | User name | trapinit | Indicates the credential that the endpoint uses to report alarms to the videoconferencing network management server. | |
| Engine ID | - | Used to authenticate trap | | |

| Parameter | | Default Setting | Description | Remarks |
|-----------------------------------|-------------------------|-----------------|---|---|
| | | | information reported by the endpoint. | |
| | Authentication protocol | SHA | Indicates the authentication mode and password for connecting the videoconferencing network management system to your endpoint. | |
| | Authentication password | Change_Me | | |
| | Encryption protocol | AES | Indicates the encryption protocol and password for connecting the videoconferencing network management system to your endpoint. | |
| | Encryption password | Change_Me | | |
| SNMPv3 Authentication information | User name | v3user | Indicates the credential that the videoconferencing network management server uses to obtain endpoint settings. | When the videoconferencing network management server is used as a client, the parameter settings must be the same as those on the endpoint. |
| | User rights | Read and write | Indicates the rights that the videoconferencing network management server uses to obtain endpoint settings. | |
| | Authentication protocol | SHA | Indicates the authentication mode and password for connecting the videoconferencing network management system to your | When the videoconferencing network management server is used as a client, the parameter settings must be the same |
| | Authentication password | Change_Me | | |

| Parameter | | Default Setting | Description | Remarks |
|-----------|---------------------|-----------------|---|--|
| | | | endpoint. | as those on the endpoint. When the videoconferencing network management system attempts to connect to your endpoint, Authentication protocol and Authentication password set on your endpoint are required. |
| | Encryption protocol | AES | Indicates the encryption protocol and password for connecting the videoconferencing network management system to your endpoint. | When the videoconferencing network management server is used as a client, the parameter settings must be the same as those on the endpoint. |
| | Encryption password | Change_Me | | |

Wi-Fi Hotspot Names and Passwords

When the Wi-Fi hotspot function is enabled on the endpoint, other devices, such as tablets, and PCs, can access a Wi-Fi network by connecting to the endpoint.



NOTE

Before using the Wi-Fi hotspot function, ensure that the Wi-Fi function is enabled and functions properly. To improve device security, set a password at your first login and regularly change the password afterward.

Table 10-4 describes the Wi-Fi hotspot names and passwords.

Table 10-4 Wi-Fi hotspot names and passwords

| Wi-Fi Hotspot Name | Default Setting | Description | Remarks |
|--------------------|-----------------|-------------|---------|
| | | | |

| Wi-Fi Hotspot Name | Default Setting | Description | Remarks |
|--------------------|---|--|--|
| TEX0_wifi_ap | The required password varies depending on your setting of Encryption mode . If you set Identity authentication mode to OPEN and Encryption mode to NONE , the Wi-Fi network provided is open to everyone. In other circumstances, the default password is Change_Me . To ensure account security, do not set Identity authentication mode to OPEN . | The devices, such as tablets, and PCs, can access a Wi-Fi network by connecting to the endpoint. | On the web interface, change SSID Number and Password of the Wi-Fi hotspot as follows: Choose System Settings > Network > Wi-Fi Settings , enable Wi-Fi Hotspot , and set SSID Number and Password . |

**NOTE**

If you set **Identity authentication mode** to **OPEN** or **WPA-PSK**, the authentication or encryption mode may result in security risks. Therefore, **WPA2-PSK** is recommended.

Wi-Fi Hotspot Whitelist

To enhance connection security, configure the Wi-Fi hotspot whitelist.

**NOTE**

Before configuring the Wi-Fi hotspot whitelist, ensure that Wi-Fi hotspots have been enabled.

Configure the Wi-Fi hotspot whitelist as follows:

1. Choose **System Settings > Network > Wi-Fi Settings**, and click the **Wi-Fi hotspot** tab.
2. Click **Whitelist**.
3. Select **Enable**.
You can modify the whitelist only after selecting **Enable** here.
4. Click **Add** and add **MAC address**.
5. Click **OK**. The settings take effect immediately.

10.2.2 Restoring Systems to Default Settings

If you forget the passwords, restore the system (including the passwords) to its default settings.

When the endpoint is running, press and hold the **RST** button for 10s to restore to factory defaults. After you press and hold the **RST** button for 3s, the system will prompt you that your endpoint will restore to factory defaults if you press and hold this button for 10s.

During startup, press and hold **Power** and **RST** buttons at the same time for 5s to restore to factory defaults.

10.2.3 Configuring Encryption

You can enable encryption to improve video communication security.

Background

On an IP network that is neither quality-guaranteed nor secure, encryption can be used to increase the video communication security, but may decrease communication efficiency. Both parties involved in communication must support encryption; otherwise, encryption fails. To improve communication security, you are advised to enable encryption.

Before initiating a Session Initiation Protocol (SIP) encrypted conference, you are advised to enable encryption and Transport Layer Security (TLS) registration to improve communication security.

Procedure

To configure encryption on the web interface:

1. Log in to the web interface, choose **System Settings > Security > Encryption** and configure the encryption mechanism.
 - **Not encrypted:** No stream is encrypted.
 - **Force encryption:** Streams are forced to be encrypted. If you select this option, your endpoint can attend encrypted conferences only. To improve communication security, select this option.
 - **Automatic encryption:** endpoint uses the appropriate encryption policy and algorithm to encrypt streams. Streams are encrypted only when a call is set up. If you select this option for the local site and encryption is disabled at a remote site, the conference between the local and remote sites is not encrypted.
2. Click **Save** for the settings to take effect immediately.

10.2.4 Web Management Users

You can manage **admin** and **api** user names and passwords on the web interface.

Background

admin and **api**: administrators with the same rights

Logging In to the Web Interface

The endpoint supports logins in HTTP and HTTPS modes. HTTPS mode, which is more secure, is used by default. If you use HTTP to log in to the web interface of the endpoint, the system automatically switches to the HTTPS mode.

Step 1 Open a browser on the computer. In the address box, enter the IP address, such as **https://192.168.1.1**.

Step 2 Press **Enter**.

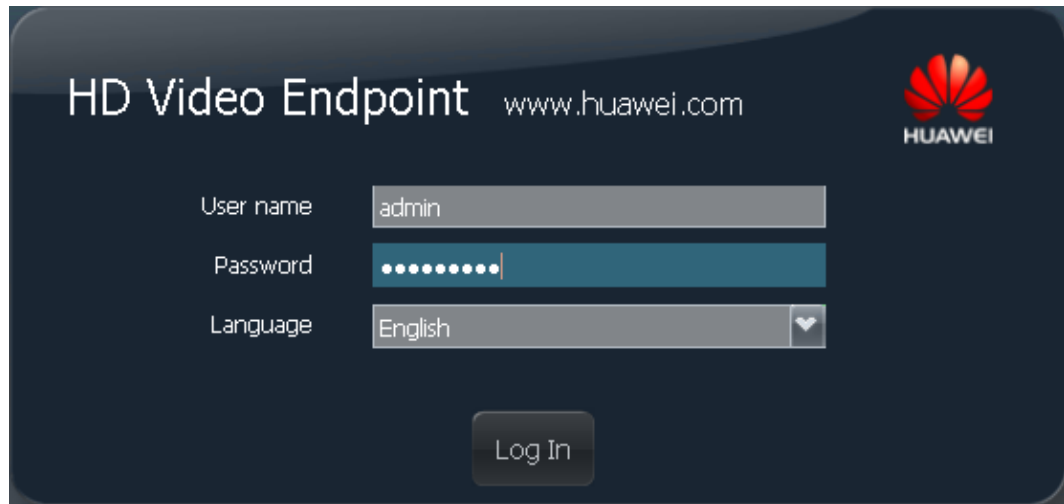
The login page is displayed, as shown in Figure 10-1.



NOTE

If the security certificate is invalid, click **Continue to this website** to resume the login.

Figure 10-1 Web login page



Step 3 Enter the user name and password. Select a **language**.

Step 4 Click **Log In**, or press **Enter**.



NOTE

To ensure data security, after accessing the web interface, close the browser and delete browser caches.

----End

Changing the User Name and Password

You can change the passwords of **admin** and **api** accounts on the web interface.

Step 1 Choose **System Settings > General > Personal**.

Step 2 Change the account password.

- The password contains at least eight characters.
- The password must contain at least three types of the following: uppercase letter, lowercase letter, digit, or special character.
- The password cannot contain more than two consecutive characters that are the same.

Step 3 Click **Save**.

----End

10.2.5 Web Access Control

The endpoint adopts HTTPS mode, which is the secure version of Hypertext Transfer Protocol (HTTP).

With the web access control function, the endpoint:

- Allows the user to submit the log out application.
When you have logged in to the web interface, you can click **Exit** in the upper right corner. The login interface is displayed.
- Allows at most 10 users to use the same or different accounts to log in to the web interface concurrently.

If the number of user attempts to log in to the endpoint web interface reaches a predefined number, the user account will be locked and cannot be used for login until the locking duration ends. On the web interface, choose **System Settings > Security > Web Login**, and set **Maximum login attempts** and **Lock time**.

10.2.6 SSH Access Control

During remote access and data transmission, SSH commands can be run to create an encrypted channel between the application layer and client.

Enabling SSH or Telnet

Telnet is an insecure communication protocol. You are advised to disable Telnet login. To enable Telnet login, choose **System Settings > Security > SSH/Telnet** on the web interface to enable SSH or Telnet.

User Login

Following describes SSH access control methods using the PuTTY as an example.



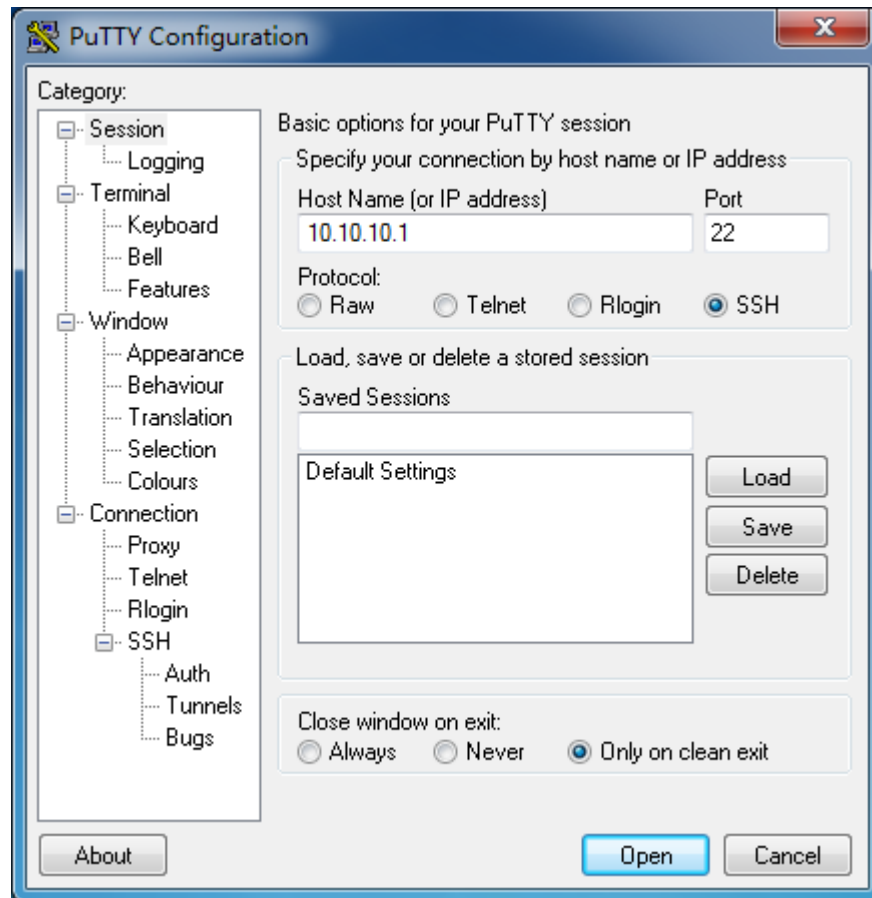
NOTE

PuTTY is a login application for remote login across different platforms. It can be obtained from Huawei Unified Communications and Collaboration (UC&C) Security Center by Huawei technical support or downloaded from the Internet. Use PuTTY 0.63 or a later version.

Step 1 Run PuTTY on your computer.

The PuTTY Configuration dialog box is displayed, as shown in Figure 10-2.

Figure 10-2 PuTTY Configuration dialog box



Step 2 In **Host Name (or IP address)**, enter the IP address, such as **10.10.10.1**.

Step 3 Select **SSH** for **Protocol**. Use the default value for **Port**.

Step 4 Click **Open**.

Step 5 Enter the user name and password and run the commands. For details, see the Command Reference of the product.

 **NOTE**

For default Telnet and SSH user names and passwords, see 10.2.1 Application Layer Account List.

----End

10.2.7 Viewing Logs

Viewing logs on the web interface helps you maintain the system, locate faults, and perform auditing tasks.

Logs of the web interface record all non-query events during the endpoint operation, including user activities and commands. The logs help you maintain the system, locate faults, and perform auditing tasks.

Step 1 Log in to the web interface and choose **Maintenance > Logs**.

- Step 2** On the **Logs** page, click **Export**.
 - Step 3** Click **Save** in the displayed dialog box.
 - Step 4** Choose the folder to save the logs and click **Save**.
 - Step 5** Open the exported logs using the Internet Explorer.
- End

10.2.8 Enabling FTPS

The endpoint supports File Transfer Protocol over SSL (FTPS) and File Transfer Protocol (FTP). To improve communication security, enable FTPS. After the network address book is enabled, the endpoint enables FTPS by default.

On the web interface, choose **System Settings > Network > Address Book > FTP address book**, and enable or disable FTPS.

10.2.9 Configuring an FTPS Server

FTPS is an extension of the commonly used FTP to support the SSL. The FTPS server ensures the security of the endpoint network address book.



NOTE

To configure the network address book after the FTPS client is configured, see the 6 Address Book Management.

Following uses the FileZilla server as an example to describe how to configure an FTPS server.


- Step 1** Set the IP address of the computer on which the FTPS server (for example, FileZilla server) is to be installed. Ensure that the IP addresses of the computer and endpoint are in the same network segment.
- Step 2** Run the FTPS server installer (for example, FileZilla_Server-0_9_41.exe) to install the FTPS server on the computer.
- Step 3** Double-click  to run the FTPS server. Click **OK** in the displayed dialog box, as shown in Figure 10-3.

Figure 10-3 Connect to Server dialog box



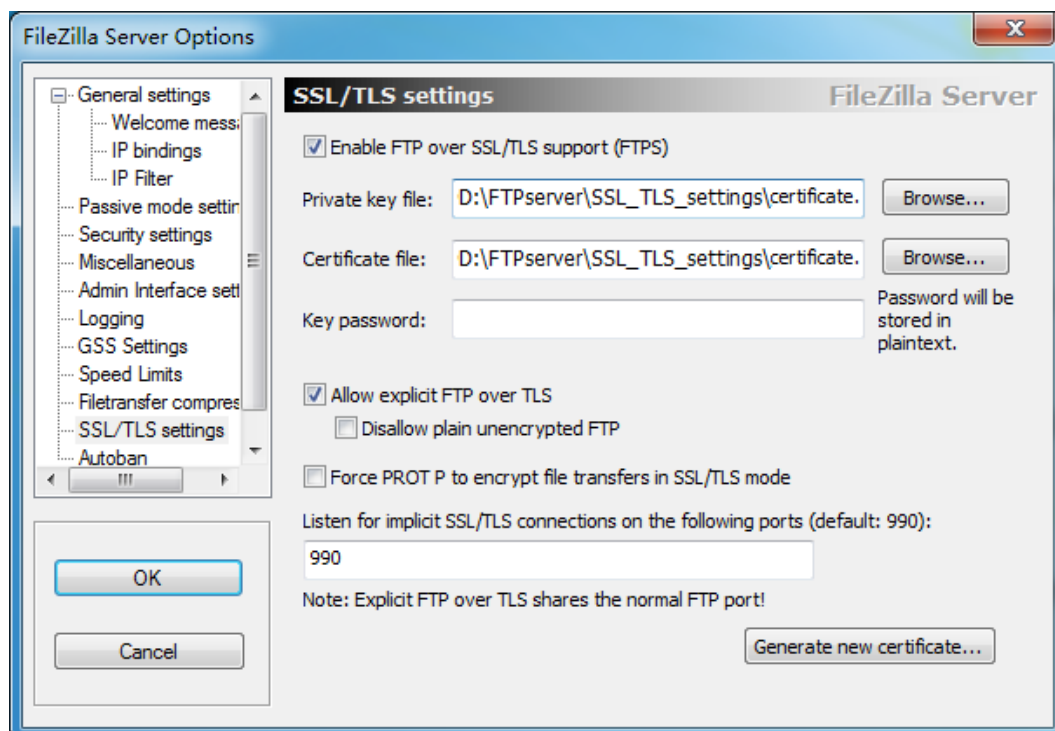
Step 4 Choose **Edit > Settings**.

Step 5 Click **SSL/TLS settings** in the left column and select **Enable FTP over SSL/TLS support (FTPS)**, click **Browse** to import the certificate, and click **OK**, as shown in Figure 10-4.

NOTE

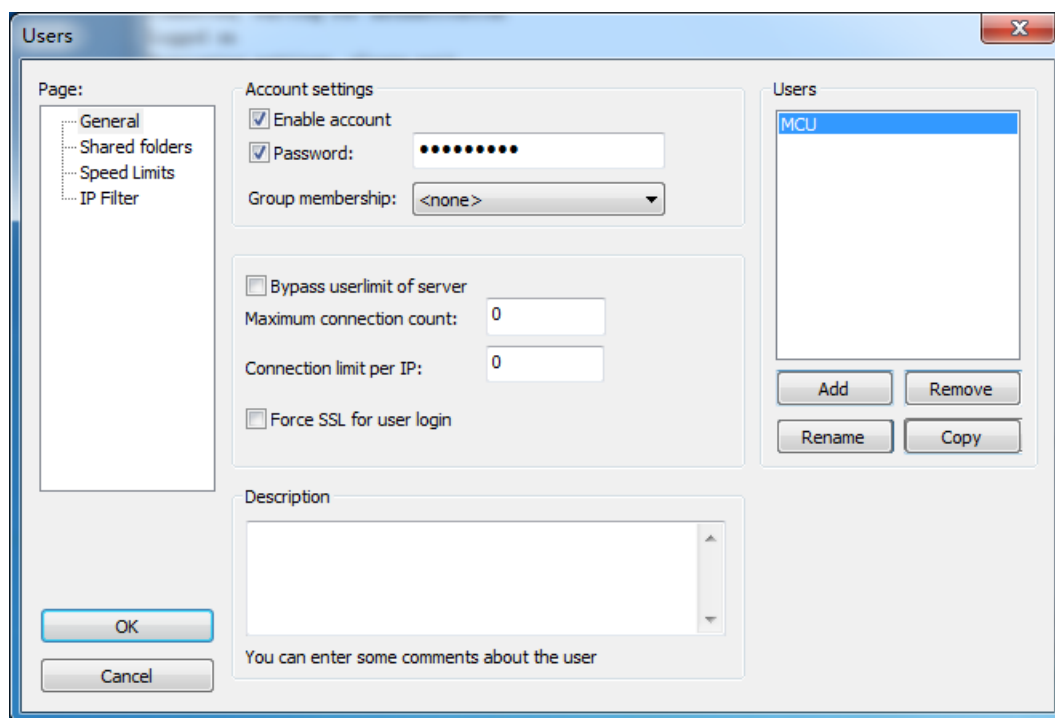
- Before importing a certificate, make sure it is issued by a security authority to prevent security risks.
- If no certificate is available, click **Generate new certificate**.

Figure 10-4 FTPS Server Options dialog box



Step 6 Choose **Edit > Users**. The Users dialog box is displayed, as shown in Figure 10-5.

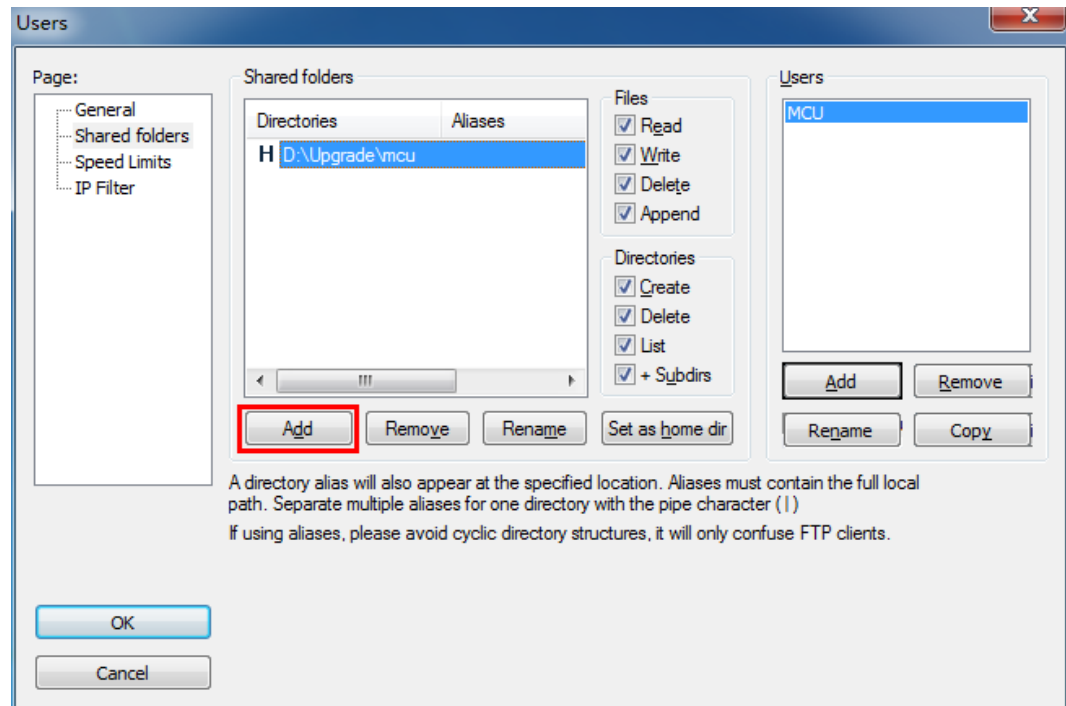
Figure 10-5 Adding a user



Step 7 Click **Add** to add a user. Select **Enable account** and **Password** and enter the **Password**.

Step 8 Click **Shared folders** under **Page**, then click **Add**, and set the path for the user root directory of FTPS server, as shown in Figure 10-6.

Figure 10-6 Specifying the path for the user root directory of FTPS server



Step 9 Click **OK**.

----End

10.2.10 Managing Certificates

You can import server and CA certificates into your endpoint on the web interface. These certificates can be used to identify users, certificate authorities, and servers to improve communication security. For example, if an endpoint needs to register with a SIP server using the Transport Layer Security (TLS) protocol or encrypts BFCP signaling over TLS, it must have a server certificate loaded first.



NOTICE

Before importing a certificate, make sure it is issued by a security authority to prevent security risks.

- **Server Certificate:** You have obtained the required certificate from the SIP server administrator or downloaded it from a certificate authority.
- **CA Certificate:** You have downloaded the required certificate from a certificate authority.

Step 1 Choose **Maintenance > Certificate Management**.

The **Certificate Management** page is displayed.

Step 2 Choose the **Server Certificate** or **CA Certificate** tab, and click **Add Certificate**.

The **Import Certificate** dialog box is displayed.

Step 3 Click **Select File** to select the certificate you want to import.

Step 4 Select the desired certificate type.

Step 5 Click **Import**.

Step 6 Click **Return** when **OK** is displayed.



NOTE

After adding a certificate, you can delete it or view its details. For a server certificate, you can also enable or disable the HTTPS, SIP, and 802.1X services for it.

----End

10.2.11 Importing and Updating Web Certificates

To help ensure communication security, import web certificates, including the trusted Certificate Authority (CA) file, local certificate file, local private key file, and local private key password file, to the endpoint through the endpoint web interface.

Importing Web Certificates



NOTICE


Professional guidance is required for importing certificates. Make sure the certificate to be imported matches the certificate type selected; otherwise, the endpoint may malfunction.

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import Web Certificate**.

The **Import Web Certificate** dialog box is displayed.

Step 3 Click  and select a certificate type.

Step 4 Click , select the certificate you want to import, and click **Import**.

Step 5 Click **Return** when **OK** is displayed.

----End

Updating Web Certificates

Update imported web certificates for them to take effect.

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Update Web Certificates**.

Step 3 Click **OK**.

The endpoint restarts.

----End

10.2.12 Importing and Exporting Settings

You can configure endpoints in batches by importing the configuration file on the web interface (exporting supported also) or from a USB device.

Importing and Exporting Settings on the Web Interface

You can import or export settings on the endpoint web interface to a configuration file. After your endpoint is restored to its default settings, you can import previously exported settings from the configuration file.



NOTE

Keep the configuration file safe to prevent disclosure of personal information.

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import/Export Settings**.

The **Import/Export Settings** page is displayed.

Step 3 Click **Import Settings** to import or **Export Settings** to export system settings.

The web administrator password is required when you import the configuration file. After the configuration file is imported successfully, the endpoint automatically restarts for the configuration file to take effect.

----End

Importing Settings on the USB Device

Step 1 Use the USB configuration tool to import the configuration file to a USB device.

Step 2 Insert the USB device into the endpoint's USB port.

Step 3 Using the remote control, enter the administrator password as prompted.

The endpoint restarts automatically.



NOTE

When compressing the configuration file, set the password to the same as the administrator password for the remotely controlled UI; otherwise, the configuration file cannot be imported to your endpoint. If the administrator password for the remotely controlled UI is empty, set the password to **12345678**, which is the default password for the remotely controlled UI administrator.

Step 4 After the restart is complete, remove the USB device.

----End

10.3 System Layer Security

Security maintenance of the system layer is to ensure a smooth operation of the operating system, which can support the operation of application layer.

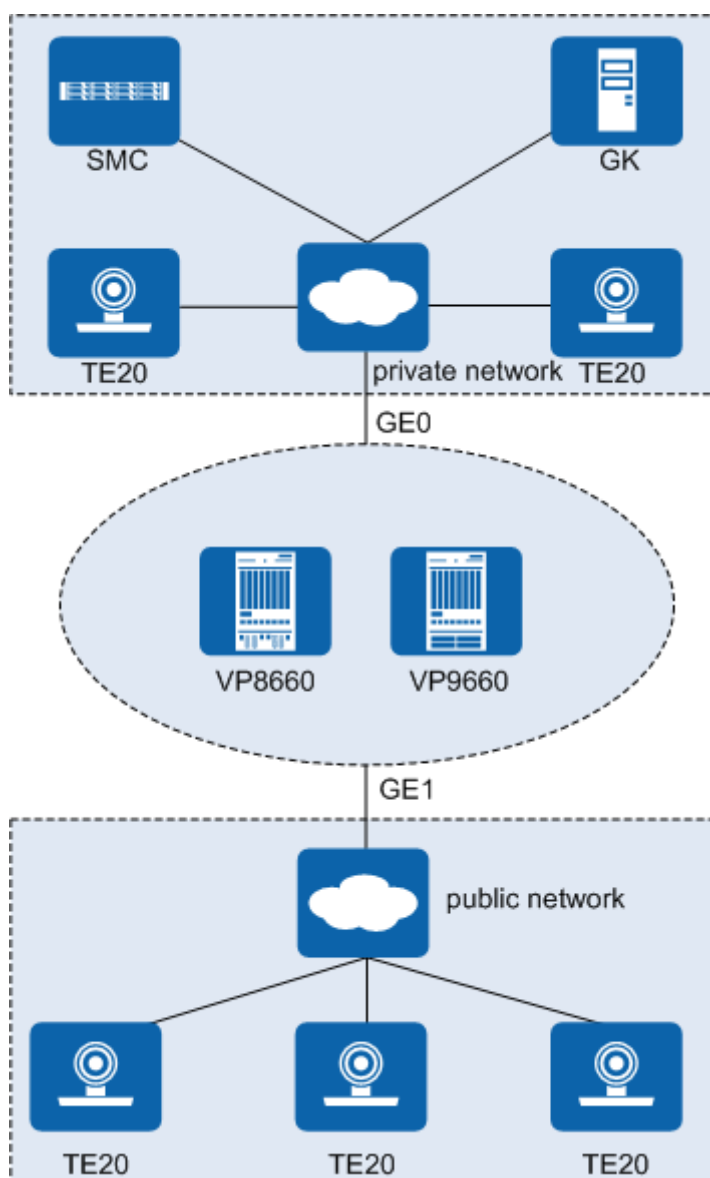
The endpoint uses Linux, which is more secure and immune to viruses than Windows.

Patches are released regularly. To improve system security, it is recommended that users download latest patches at <http://e.huawei.com> regularly and apply them after performing antivirus checks.

10.4 Network Layer Security

On an endpoint security network, the endpoint on the private network connects to the GE0 port on the MCU, while the endpoint on the public network connects to the GE1 port on the MCU, which implements network isolation and fortifies network layer security.

Figure 10-7 shows the TE10 security network.

Figure 10-7 TE20 security network

Over the network:

On this network, the endpoint is connected to the Multipoint Control Unit (MCU) through the private network, which connects to different networks through different ports. The endpoint on the private or public network can join the conference even if the call protocol or the firewall settings (such as enabled ports) are not changed.

10.5 Management Layer Security

To ensure management layer security, you are advised to comply with security principles and suggestions for system maintenance, log recording, signaling diagnosis, security assessment, touch panel hardening, data backup, defect feedback, attack defense, and security emergency response.

10.5.1 Principles of System Maintenance Security

It is recommended that you comply with account management, permission management, and auditing principles to ensure system maintenance security.

Account Management

- Manage the accounts strictly.
- Control the permissions of accounts of different levels. Only users of higher levels can change the passwords for users of lower levels.

Permission Management

- Minimize permissions to the system service and permissions of accounts.
- Strictly control the operation authorization on the web interface.

Auditing Principles

- Use logs and other feasible methods to monitor operations on the endpoint.
- Audit the failed access to the system's important resources.
- Audit the successful access to the system's important resources.
- Audit the failed and successful access control strategy modification.

10.5.2 Guidelines for Password Security Maintenance

User identities must be authenticated before users can log in to application systems. The complexity and validity periods of accounts and passwords can be configured according to system security requirements.

Guidelines for password security maintenance are as follows:

- Change the password periodically to prevent risks.
- Designate specialist personnel to manage the administrator account and password.
- Encrypt passwords during data transmission.
- Remind users to change their passwords after system deployment.
- Change passwords periodically. Do not use the default passwords or old passwords used last five times.

10.5.3 Log Maintenance Suggestions

It is recommended that you take log maintenance suggestions and utilize logs to help find errors.

The system must record the operations, such as system parameter settings and conference calls in the logs. Reinforce the system to protect the logs.

Checking Logs Regularly

Check the system logs, applications logs, and security logs regularly and report to the department of a higher level once abnormal logs are found. Ask the local representative office for help if the issues cannot be located or resolved.

Backing Up Logs Regularly

Back up logs regularly by exporting them manually and store the logs on devices, such as the disc, tape, or compact disc. The system supports a maximum of 80 MB logs. Once the size of logs exceeds 80 MB, new logs will replace the old ones. In this case, users must back up timely.

10.5.4 Guidelines on Signaling Diagnosis

To ensure information security, it is recommended that you comply with relevant laws and regulations to diagnose signaling.

You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected. The signaling diagnostics on the endpoint may contain personal information. To protect information security, make sure that your account is secure and properly managed. Use the signaling diagnostics only for problem identification and delete them immediately after use.

10.5.5 Security Evaluation Recommendations

You are advised to look for a qualified organization to evaluate the system security and contact Huawei technical support engineers when problems occur during the evaluation.

10.5.6 Backup Suggestions

Take the backup suggestions given in this section to ensure security.

In the following scenarios, back up the logs to ensure security.

- Before daily security maintenance, and before and after the system troubleshooting.
- Before patch installation and upgrade.

For details about the upgrade, see the section 9.9 Backup and Restoration.

10.5.7 Defect Feedback Suggestions

It is recommended that you give feedback to Huawei once a security incident happens when the endpoint is used.

Huawei will take the following actions accordingly:

- If a security incident happens, Huawei technical support engineers will support customers remotely or onsite to reduce the impact on the system and improve the report on the accident treatment.
- If no security incident happens, Huawei technical support engineers record defects in to the database and send to the R&D team. Once the R&D team prescribes a solution, the technical support engineers will analyze the solution's possible impact on the site operations and provide a final solution.

10.5.8 Common Measures Against Attacks

The system can defend against up to 200 common attacks. The measures defending against these attacks are described in this section.

- Deploy firewall devices on the network where the endpoint is located.

- Disable protocols that may impose attacks, such as Telnet and SSH. By default, Telnet and SSH are disabled.
To prevent devices from attacks, it is recommended Telnet and SSH be disabled. To disable Telnet and SSH, on the endpoint web interface, choose **System Settings > Security > SSH/Telnet** and set both **SSH** and **Telnet login** to **Do not allow**.
- If the endpoint is deployed on a public network, power off the endpoint when it is not in use.
- Add frequently-used IP addresses or IP address segments to the whitelist. This approach helps defend against potential network threats, such as flood attack and slow HTTP attack. For details, see System Connection Whitelist.
- Periodically backup system configuration files to restore the system if an exception occurs. For details, see 9.9 Backup and Restoration.
- Check device alarms every day and clear unnecessary alarms in time to ensure proper running of the system. For details, see 9.6 Checking Alarms.
- Periodically check and back up logs and find error information from them. For details, see 10.2.7 Viewing Logs.

10.5.9 Security Emergency Response Mechanism

Users need to build a security emergency response mechanism to ensure that the system can immediately respond to security issues and return to proper operations to minimize losses.

10.5.10 Security Emergency Response Mailbox

You can contact the Huawei Product Security Incident Response Team (PSIRT) via the security emergency response mailbox when encountering an emergency.

Contact the Huawei PSIRT via PSIRT@huawei.com if you wish to:

- Provide feedback on vulnerabilities of Huawei products.
- Obtain emergency response service from Huawei.
- Obtain information about vulnerabilities of Huawei products.

Encrypt the files that contain sensitive information before sending them. Go to <http://www.huawei.com/en/security/psirt/about-huawei-psirt/index.htm> to obtain the encryption key.

11 Troubleshooting

This chapter describes how to diagnose and troubleshoot endpoint faults.

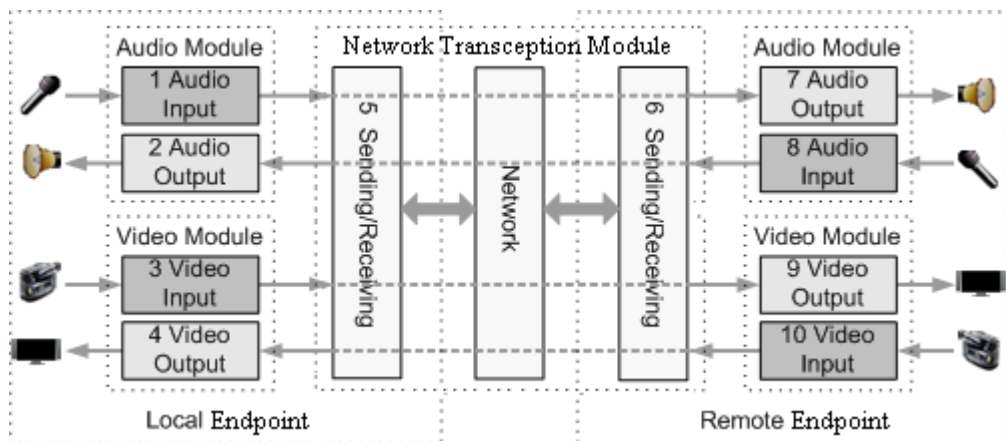
11.1 Fault Diagnosis

The endpoint supports the following diagnosis methods: sound and color bar tests, loopback tests, network tests, one-click diagnosis, signaling diagnosis, and tracer.

11.1.1 Fault Diagnosis Model

Figure 11-1 shows the diagnosis model for your endpoint.

Figure 11-1 Diagnosis model



According to Figure 11-1, diagnosis functions diagnoses the audio module, video module, and network module.

Audio signals are transmitted in the following paths:

- Local microphone → 1 → 5 → Communications network → 6 → 7 → Remote speaker
- Local speaker ← 2 ← 5 ← Communications network ← 6 ← 8 ← Remote microphone

Video signals are transmitted in the following paths:

- Local camera → 3 → 5 → Communications network → 6 → 9 → Remote monitor
- Local display ← 4 ← 5 ← Communications network ← 6 ← 10 ← Remote camera

11.1.2 Fault Diagnosis Methods

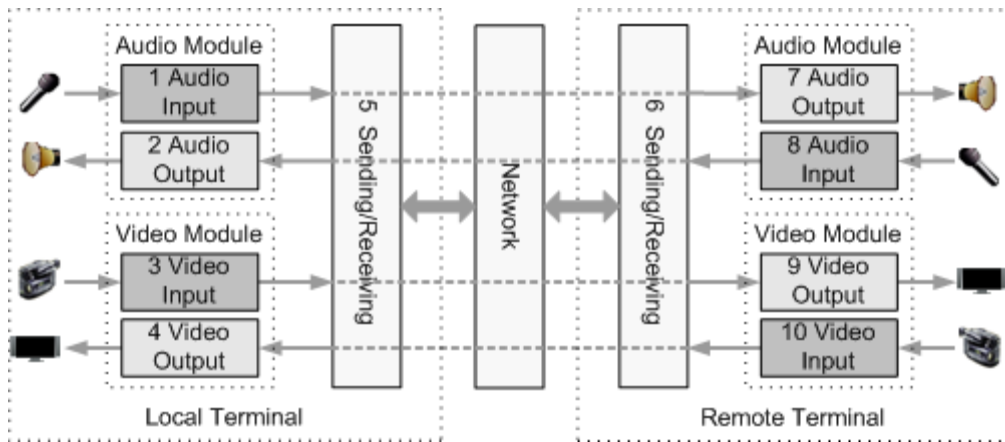
With the diagnosis file functions on your endpoint, you can perform sound, color bar, loopback, network tests, one-click diagnosis, signaling packet capture, and route test.

NOTE

You can use either of one-click trace diagnosis and signaling diagnosis at a time.

Figure 11-2 shows the diagnostic model for your endpoint.

Figure 11-2 Diagnostic model



According to Figure 11-2, diagnosis functions diagnose the audio module, video module, and network module.

Audio signals are transmitted in the following paths:

- Local microphone → 1 → 5 → Communications network → 6 → 7 → Remote speaker
- Local speaker ← 2 ← 5 ← Communications network ← 6 ← 8 ← Remote microphone

Video signals are transmitted in the following paths:

- Local camera → 3 → 5 → Communications network → 6 → 9 → Remote monitor
- Local display ← 4 ← 5 ← Communications network ← 6 ← 10 ← Remote camera

Sound and Color Bar Tests

Table 11-1 lists the sound and color bar tests.

Table 11-1 Sound and color bar tests

| Test | Item to Be Tested | Signal Stream |
|-----------|-------------------|---------------|
| Sound | 2 audio output | 2 → Speaker |
| Color bar | 4 video output | 4 → Monitor |

- Sound test: Choose **Maintenance > Diagnostics**. On the **Diagnostics** page, click **Sound Test**. While the test audio stored on your endpoint plays, check the sound quality.
- Color bar test: Choose **Maintenance > Diagnostics**. On the **Diagnostics** page, click **Color Bar Test**. Seven color bars are shown on the display for you to check the color quality.

Loopback Test

Your endpoint can transmit audio or video data on a channel to simulate an actual application and test whether the output is satisfactory. You can perform a local loopback test to check the local network connection or a remote loopback test to check the remote network connection. When you perform a remote loopback test, data is transmitted from your site to a remote site, and then back to your site. Table 11-2 lists the types of loopback tests available on your endpoint.



CAUTION

- To enable your endpoint to communicate with other endpoints, stop the loopback test.
- You cannot perform a loopback test on remote video if you are in a dual-stream conference.

Table 11-2 Loopback tests

| Test | Item to Be Tested | Signal Stream |
|-----------------------|---|--|
| Audio loopback | Local audio module | Microphone → 1 → 2 → Speaker |
| Video loopback | Local video module | Camera → 3 → 4 → Monitor |
| Remote audio loopback | <ul style="list-style-type: none"> • Remote audio module • Network transmission | Microphone → 1 → 5 → 6 → 7 → 8 → 6 → 5 → 2 → Speaker |
| Remote video loopback | <ul style="list-style-type: none"> • Remote video module • Network transmission | Camera → 3 → 5 → 6 → 9 → 10 → 6 → 5 → 4 → Monitor |

Network Test

Table 11-3 Network test

| Test | Item to Be Tested | Signal Stream |
|---------|-------------------|----------------------------------|
| Network | IP access | endpoint → LAN or public network |

Before a test, verify that the LAN network port indicator is green, which indicates that your endpoint is correctly connected to an IP network.

- In **IP address**, enter an IP address that is in a different network segment from your endpoint IP address. Then click **Start**. If the test succeeds, the gateway settings and IP address of your endpoint are correct.
- If your endpoint is on a private network, in **IP address**, enter a public IP address. Then click **Start**. If the test succeeds, the gateway settings, NAT address, and IP address of your endpoint are correct.

Route Test

A route test helps determine the path that a data packet at the network layer uses to access a destination address.

Step 1 Choose **Maintenance > Diagnostics > Tracert**.

Step 2 Set the parameters listed in Table 11-4.

Table 11-4 Route parameters

| Parameter | Description | Setting |
|--------------------|---|---------------------|
| IP address | Specifies the IP address of the destination device. | Example: 10.10.10.1 |
| Maximum hops | Specifies the maximum allowed hops. | Example: 5 |
| Timeout period (s) | Specifies the timeout period for the call waiting time, in seconds. | Example: 1 |

Step 3 Click **Start** to start route test.

----End

One-Click Diagnostics

Web administrators and API users can perform one-click diagnosis on the endpoint. The diagnosis file helps with fault identification.

Step 1 Choose **Maintenance > Diagnostics > One-Click Diagnostics**.

Step 2 Click **One-Click Diagnostics**.

The **One-Click Diagnostics** dialog box is displayed.

Step 3 Select the module to diagnose and click **Start**.

The diagnosis takes about 5 minutes.

 **NOTE**

If you have selected **Error report**, a dialog box will be displayed on the remote control UI after you click **Start**. In this case, select **Yes**. Then, the diagnosis starts.

Step 4 Click **Download** to save the diagnosis file to the local computer.

 **NOTE**

If you have selected **Error report**, a dialog box will be displayed on the remote control UI after you click **Download**. In this case, select **Yes**. Then, the system starts downloading the diagnosis file.

----End

Signaling Diagnostics

Web administrators and API users can perform signaling diagnosis and export the diagnosis file from the endpoint web interface. The diagnosis file helps with fault identification.

 **NOTE**

- Only one user can perform signaling diagnosis.
- Signaling diagnosis can last at most 10 minutes. Even if you do not click **Stop**, signaling diagnosis will automatically stop in 10 minutes from the time when the diagnosis starts. The diagnosis file cannot exceed 10 MB.

Step 1 Choose **Maintenance > Diagnostics > Signaling Diagnostics**.

The **Signaling Diagnostics** dialog box is displayed.

Step 2 Click **Start** to start signaling diagnosis.

When prompted, click **OK**.

 **NOTE**

Signaling diagnosis does not monitor media stream data, but will obtain site information, such as site numbers. Perform this operation with caution.

Step 3 Click **Stop** to stop signaling diagnosis.

Step 4 Click **Download** to save the diagnosis file to the local computer.

----End

11.2 Common Faults

This section describes the problems you might encounter when using your endpoint and provides solutions.

11.2.1 Web Interface

Table 11-5 lists the troubleshooting methods for problems that may arise on the endpoint web interface.

Table 11-5 methods for troubleshooting endpoint web interface problems

| Problem | Possible Cause | Solution |
|---|---|---|
| A message is displayed to indicate that your endpoint failed to connect to the Internet or download | The latest patches for the operating system or Internet Explorer are not installed. | Install the latest patches for the operating system and Internet Explorer. |
| | The security level of Internet Explorer is too high, or your endpoint IP | 1. From the Internet Explorer menu bar, choose Tools > Internet Options . 2. Click the Security tab, Trusted sites , |

| Problem | Possible Cause | Solution |
|---|--|--|
| images. | address has not been added to the list of trusted sites. | and then Sites . 3. In Add this Web site to the zone , enter your endpoint IP address. Then click Add . 4. Click OK . |
| Button text is not fully displayed. | Internet Explorer is set to ignore the font styles specified on web pages. In this case, the font specified by your endpoint cannot be recognized. | 1. From the Internet Explorer menu bar, choose Tools > Internet Options . 2. Under Appearance on the General tab, click Accessibility . 3. In the Accessibility dialog box, deselect all options. 4. Click OK . |
| The records of the local address book cannot be exported. | The pop-up blocker is enabled on your browser. | <ul style="list-style-type: none"> • If Internet Explorer is used: On the Internet Explorer menu bar, choose Tools > Pop-up Blocker > Turn Off Pop-up Blocker. • If the Firefox is used: Choose Tools > Options. On the General tab, select Show the Downloads window when downloading a file. On the Privacy tab, select Accept cookies from sites. Then click OK to save the settings. |

11.2.2 Network

Table 11-6 lists the troubleshooting methods for problems that may arise on the network.

Table 11-6 Methods for troubleshooting common network problems

| Problem | Possible Cause | Solution |
|---|--|-------------------------------------|
| When you attempt to use Telnet to access the endpoint, a message is displayed to indicate that the number of connections to the endpoint has reached the limit. | <p>The number of connections to the endpoint has reached the maximum value.</p> <p>NOTE</p> <ul style="list-style-type: none"> • A maximum of three SSH and Telnet connections to the endpoint is allowed. • A maximum of three SSH connections to the endpoint is allowed. | Disconnect some Telnet connections. |

NOTE

By default, the Telnet service is disabled. The Telnet service is generally used to query system status and logs and perform specific maintenance. Exercise caution when enabling this service.

11.2.3 Video

Table 11-7 lists the troubleshooting methods for video problems.

Table 11-7 Methods for troubleshooting video problems

| Problem | Possible Cause | Solution |
|--|---|--|
| While the endpoint is powered on and not in a conference, the display device does not display the remote controlled UI or the video of your site. | The display device is powered off. | Power on the display device. |
| | The video channel of the display device is incorrect. | Use the remote control to select the correct video channel. |
| | The video settings of the endpoint or display device are incorrect. For example, the brightness is set to 0. | Retain the default values for the video parameters on the endpoint and display device. |
| | The video cable connection is not secure. | Secure the video cable between the endpoint and display device. |
| | The monitor does not support the video output settings configured on the endpoint. | On the web interface, choose System Settings > Input/Output > Video Output , and set the appropriate parameters again. |
| | The video output settings configured on the endpoint are inconsistent with the actual connections. | On the web interface, choose System Settings > Input/Output > Video Output based on the actual connections on the endpoint, and set the appropriate parameters again. |
| While the endpoint is powered on and not in use during a conference, the display device displays the video of your site but cannot display the remote controlled UI. | The endpoint does not respond to remote control operations. | Telnet to the endpoint. If you fail to operate the endpoint, it is malfunctioning. In this case, restart the endpoint. If the problem persists, contact the local distributor for maintenance. |
| While the endpoint is in use during a conference, the display device displays the video of your site but cannot display the video | A local or remote loopback test is being performed. | Stop all local and remote loopback tests. |
| | Check the call statistics. If the value of Video bandwidth[frame rate] is 0 , no video is sent from remote sites. | Contact the remote site administrator to resolve this problem. |

| Problem | Possible Cause | Solution |
|---|--|--|
| of any remote site. | If the remote video is displayed as a blue screen, the remote site is blocking its video by sending a blue screen. | Contact the remote site administrator to resolve this problem. |
| | The video output port is set to display the video of your site. | Set the video output port to display the video of a remote site. |
| | Local video is turned off by a remote site. | Ask the administrator of the remote site to turn on the local video. |
| | It is a voice-only conference. | - |
| The video of your site is in black and white or flickers in black and white. | The mode adopted by the video output port is set incorrectly. | <ul style="list-style-type: none"> Replace the cable if necessary. |
| While the endpoint is in use during a conference, the video of a remote site is not clear. For example, there are artifacts, frozen images, or discontinuity in the video output. | Faults occur in the local video module. | Perform a local video loopback test. If the video quality is poor, faults occur in the local video module. In this case, send the endpoint to the local distributor for maintenance. |
| | The remote camera is set to focus on a close or distant scene. When the remote camera is not set to automatic focus and the scene captured by a remote camera changes, the captured video becomes unclear. | Set the remote camera to automatic focus. |
| | Only low video bandwidth is available for your site because the network is busy. | Do not initiate conferences during network busy hours. |
| | The quality of a network connection device, such as an optical fiber transceiver, is poor. As a result, certain data is lost during transmission. | Replace the related network connection device. |
| | Packet loss occurs on the network. | Contact the network administrator. |
| While the endpoint is in use during a | Ask the remote site administrator to perform a local video loopback | Ask the administrator of the remote site to disconnect from the conference, set the video frame rate to a smaller value, and |

| Problem | Possible Cause | Solution |
|---|---|--|
| conference, the video of a remote site can be displayed continuously but the video quality is not satisfactory. | test. If the video quality is good, the video frame rate set at the remote site is too high. | join the conference again. |
| | Ask the administrator of the remote site to perform video loop and check video image quality. | Ask the administrator of the remote site to perform automatic camera focus. |
| While the endpoint is not in use during a conference, the video displayed on the display device is too bright or too dark. | The video settings of the endpoint are inappropriate. | Retain the default values for the video parameters on the endpoint and display device. |
| | The video settings of the display device are inappropriate. | Retain the default values for the video parameters on the endpoint and display device. |
| | The camera is faulty. | Send the endpoint to the local distributor for maintenance. |
| While the endpoint is in use during a conference and a remote site is sharing its computer desktop, the local display cannot display the shared computer desktop. | The resolution of the remote computer exceeds the maximum resolution supported by the endpoint. | Ask the remote site administrator to change the resolution and refresh rate of the remote computer to those the endpoint supports. |
| | The presentation sharing function is not enabled at your site. | On the web interface, choose System Settings > Conference > Advanced Settings and enable Presentation . |
| On the camera control screen, navigation and volume keys on the remote control are unavailable. | The camera you want to control is not selected. | Access the camera control screen and select the camera you want to control. |
| | Camera settings are incorrect. | Verify the camera settings. |
| Slight jitters occur on the demonstration video. | Because of an incorrect interface connection or transmission cable fault, VGA input signal interferences occur when the frame rate is greater than 60 fps. As a result, slight jitters occur. | On the web interface, choose Device Control > Device Control > Preference-Video , and adjust the sampling phase to resolve the fault. |

11.2.4 Audio

Table 11-8 lists the troubleshooting methods for audio problems.

Table 11-8 Methods for troubleshooting audio problems

| Problem | Possible Cause | Solution |
|--|---|--|
| Current noise is generated when the endpoint's audio output ports are connected to audio devices, such as speakers, tuning consoles, and audio matrices. | Disconnect the endpoint's audio output ports from the audio devices. Check whether the problem is rectified. If the problem persists, the current noise is caused by audio device or cable issues. | Replace the cables or repair the audio devices. |
| | If the problem is rectified, check the grounding status of the audio devices and endpoint. | <ul style="list-style-type: none"> • If the audio devices' shells are grounded, the endpoint's shell must be grounded nearby. • If the audio devices' shells are not grounded, the endpoint's shell does not need to be grounded either. Specifically, change the endpoint's AC three-core power supply to two-core power supply. |
| While the endpoint is in use during a conference, no audio is delivered from the local display device. | Perform an audio test to check whether the problem occurs at your site or a remote site. If no audio is delivered from the display device during the audio test, the problem exists at your site. | <ul style="list-style-type: none"> • If the chair site has muted the speaker of your site, contact the chair site to resolve this problem. • If the display device volume is adjusted to the lowest, restore the volume to its default value. • If the endpoint volume is adjusted to the lowest, restore the volume to its default value. • If the audio cable is connected incorrectly or insecurely, reconnect the audio cable from the endpoint to the display device. |
| | If audio is properly delivered from the display device during the audio test, the problem occurs at the remote site. | <ul style="list-style-type: none"> • The microphone at the remote site has been muted or the chair site has muted this microphone. In this case, contact the chair site to resolve this problem. • No sound pickup device, such as a microphone, is connected to the audio input port. In this case, set the audio source again or connect a sound pickup device to the corresponding port. • The related sound pickup device is powered off. In this case, power on the |

| Problem | Possible Cause | Solution |
|---|--|---|
| | | device. <ul style="list-style-type: none"> The audio cable is connected insecurely. In this case, reconnect the audio cable to the endpoint. |
| While the endpoint is in use during a conference, only the sound from your site can be delivered from the display device and you cannot hear other sites. | A loopback test is being performed at your site. | Stop all local and remote loopback tests. |

11.2.5 Conference Initiation

Table 11-9 lists the troubleshooting methods for problems you may encounter during conference initiation.

Table 11-9 Methods for troubleshooting common problems with conference initiation

| Problem | Possible Cause | Solution |
|--|--|---|
| Your site and a remote site cannot call each other using site numbers. | Your site or the remote site has not registered with an SC. An SC is responsible for translating site numbers into IP addresses. If either your site or the remote site does not register with an SC, the translation cannot be implemented, and your site cannot place a call to the remote site using the site number. If a remote site places a call to your site by site number, it will receive a message from the SC indicating that your site has not registered with the SC, and the call cannot be set up. | Verify SC registration settings and register your site and the remote site with an SC. |
| | The local or remote endpoint is not connected to an IP network. | 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the |

| Problem | Possible Cause | Solution |
|---|--|--|
| | | <p>endpoint is steady green.</p> <ol style="list-style-type: none"> On the configuration wizard screen of the remotely controlled UI, set IP network parameters correctly. |
| Your site cannot place a call to a remote site using the IP address of the remote site. | The local or remote endpoint is not connected to an IP network. | <ol style="list-style-type: none"> Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. On the configuration wizard screen of the remotely controlled UI, set IP network parameters correctly. |
| | NAT settings are incorrect. Specifically, the local endpoint is on a private network while the remote endpoint is on a public or different private network. Check whether your endpoint can communicate with a public network. If the endpoint cannot, NAT settings are incorrect. | Choose Advanced > Settings > Network > Firewall and verify NAT settings. |
| | The GK with which the local or remote endpoint registers does not support the function for placing calls using IP addresses. | Choose Advanced > Settings > Network > IP > H.323 at your site and the remote site, respectively. Then, disable GK functions. |
| After the endpoint starts, it fails to register with the GK. | The parameters (GK address, encryption password, and user name) used for GK registration are incorrect. | On the endpoint web interface, choose Advanced > Settings > Network > IP > H.323 and correct the settings. |
| | Another site with the same number as your site has already registered with the GK. | Contact the videoconferencing system administrator to check whether another site with the same number as your site has already registered with the GK. If such a site exists, change the user name of your site. |
| | The endpoint is disconnected from an IP | <ol style="list-style-type: none"> Verify that the endpoint is connected to an IP |

| Problem | Possible Cause | Solution |
|---------|---|--|
| | <p>network.</p> <ol style="list-style-type: none"> 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. 2. On the configuration wizard screen of the remotely controlled UI, set IP network parameters correctly. <ol style="list-style-type: none"> 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. 2. On the configuration wizard screen of the remotely controlled UI, set IP network parameters correctly. | <p>network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green.</p> <ol style="list-style-type: none"> 2. On the configuration wizard screen of the remotely controlled UI, set IP network parameters correctly. |
| | <p>NAT settings are incorrect. Specifically, the local endpoint is on a private network while the GK is on a public network. Check whether your endpoint can communicate with a public network. If the endpoint cannot, NAT settings are incorrect.</p> | <p>Choose Advanced > Settings > Network > Firewall and verify NAT settings.</p> |
| | <p>The GK listening port, such as port 1719, is restricted by the network firewall.</p> | <p>Contact the videoconferencing system administrator to resolve this problem.</p> |

11.2.6 Conference Control

Table 11-10 lists the troubleshooting methods for common problems you may encounter during conference control.

Table 11-10 Methods for troubleshooting conference control problems

| Problem | Possible Cause | Solution |
|------------------------------|--|--|
| While the endpoint is in use | A site in the conference is being broadcast, and | Ask the chair site to stop site broadcast. |





| Problem | Possible Cause | Solution |
|--|---|---|
| during a conference, you cannot view the desired site. | all the sites must view that site except the chair site and broadcast site. | |
| | No video is sent from the site you want to view. | Ask the related site administrator to troubleshoot the site video. |
| | The View Site function is restricted on the RM or the SMC2.0. | Contact the videoconferencing system administrator to resolve this problem. |

A Icons on the Remotely Controlled UI

The icons provided on the user interface indicate the status and settings of the system, helping you quickly understand system status and complete tasks.



Table A-1 lists concerned icons that display the connection status in the upper right corner of the remotely controlled UI. Before initiating a conference, check the status of these icons.










Table A-1 Network status icons

| Icon | Name | Indicates... |
|---|------------------------------------|---|
|  | Network disconnection | The endpoint is disconnected from an IP network. The network cable may be disconnected. |
|  | Wi-Fi connection status | The first icon indicates that the Wi-Fi network has disconnected after the Wi-Fi client is enabled. The other icon indicates the signal status of a connected Wi-Fi network. |
|  | Remote control battery status | The battery of the remote control is insufficient. |
|  | Bluetooth device connection status | The endpoint is connected with a Bluetooth device. |

When you view a video, the icons listed in Table A-2 are used to indicate the status of certain operations. During a conference, pay attention to the status of these icons to ensure that the relevant operations are performed correctly.

Table A-2 Operating status icons

| Icon | Name | Indicates... |
|---|--------------------------|--|
|  | Microphone muting status | The microphone of the local site is muted. |
|  | Speaker muting status | The speaker of the local site is muted. |

| Icon | Name | Indicates... |
|--|--|--|
|  | Encrypted conference | The current conference is an encrypted conference (with media streams encrypted). |
|  | Chair | The local site is the chair site. |
|  | Presentation sharing on the local site | The local site is sharing a presentation. |
|  | Presentation sharing on a remote site | A remote site is sharing a presentation. |
|  | Local site broadcast | The local site is being broadcast in the current conference. |
|  | Do Not Disturb | The Do Not Disturb function is enabled at the local site. |
|  | Remote site muting | A remote site is muted, and cannot be heard by the local site. |
|   | Poor network condition | Network impairments or packet loss occurs in the network where the endpoint is located..see 8.2 Customizing the Remote Control UI. |

B Requirements on Room Layout and Lighting

When using the endpoint, pay attention to your sitting posture to avoid problems associated with your back. Do not stare at the monitor screen for a long time. This may harm your eyes or blur your vision.

Layout Precautions

- Ensure that there are no large or moving objects behind you. Otherwise, the video cannot be viewed clearly.
- Do not use striped patterns as the background.
- Do not hold a conference in a room that generates a lot of echoing.
- Do not place the endpoint near a sound source.

Lighting Precautions

To ensure high video quality, do not turn the lens towards bright lights.

C Default Accounts

To better use your endpoint, get to know the default values of common user names and passwords, default IP addresses.



NOTE

To ensure account security, you are advised to change the password at the first login and regularly change the password afterward.

Table C-1 lists the default user names and passwords for the endpoint.

Table C-1 Default user names and passwords

| Item | | Default Setting |
|--|-------------------------|---|
| Administrator password for the remotely controlled UI | | 12345678. |
| Administrator user name and password for the endpoint web interface | | The default user name and password are admin and Change_Me respectively. |
| User name and password for connecting the third party (for example, a touch panel or SMC2.0) to the endpoint | | The default user name and password are api and Change_Me respectively. |
| User name and password for logging in to the endpoint in SSH/Telnet mode | | <ul style="list-style-type: none"> • Common user: The default user name and password are admin and Change_Me respectively. • Test user: The default user name and password are test and Change_Me respectively. |
| Upgrade password | | Change_Me. |
| Default IP address after the endpoint is restored to its default settings | | 192.168.1.1. |
| Account, password, and protocol required for the network management system to connect to the | User name | v3user. |
| | User rights | Read and write. |
| | Authentication protocol | SHA. |

| Item | | Default Setting |
|------------------------------------|----------------------------|----------------------|
| endpoint through SNMP V3 | Authentication password | Change_Me. |
| | Encryption protocol | AES. |
| | Encryption password | Change_Me. |
| Wi-Fi hotspot name and password | SSID Number | TEX0_wifi_ap. |
| | Password | Change_Me. |
| AirPresence desktop password | | Change_Me. |
| CPE | CPE user name | admin. |
| | CPE password | Change_Me |

D Safety Precautions

For safety purposes, carefully read through these safety precautions and observe them during operation.

Basic Precautions

- Keep the device dry and secure from collision during storage, transportation, and operation of the device.
- Do not attempt to dismantle the device by yourself. In case of any fault, contact the appointed maintenance center for assistance or repair.
- Without prior written consent, no organization or individual is permitted to make any change to the structure or safety and performance design of the device.
- While using the device, observe all applicable laws, directives, and regulations, and respect the legal rights of others.

Environmental Precautions

- Install the device strictly according to the requirements of the manufacturer.
- Place the device on a stable surface. Suspend the wall-mounted device strictly according to requirements from the manufacturer.
- Place the device in a well-ventilated place. Do not expose the device to direct sunlight.
- Do not place the device and its accessories in an area that is excessively hot or cold.
- Do not place the device near a water source or in a damp area.
- Do not place any object on the top of the device. Reserve a minimum space of 10 cm at the four sides of the device for heat dissipation.
- Do not place the device on or near inflammable materials such as foam.
- Keep the device clean, free of dust and stain.
- Keep the device away from heat source or fire, such as a radiator or a candle.
- Keep the device away from any household appliances with strong electromagnetic fields, such as a microwave oven, refrigerator, or mobile phone.

Operating Precautions

- Do not allow children to play with the device or accessories. Swallowing the accessories may be fatal.
- Use the accessories such as the power adapter and battery provided or authorized only by the manufacturer.

- Ensure that the device does not get wet. If water gets into the device, disconnect the power supply immediately and unplug all the cables connected to the device, including the power cable, telephone cable, video cable, audio cable, network cable, and serial cable, and then contact the appointed maintenance center.
- Before plugging or unplugging any cable, shut down the device and disconnect the power supply. While plugging or unplugging any cable, ensure that your hands are dry.
- Do not step on, pull, or overbend any cable. Otherwise, the cable may be damaged, leading to malfunction of the device.
- Do not use old or damaged cables.
- In lightning weather, disconnect the device from the power supply and unplug all the cables connected to the device.
- Keep the power plug clean and dry, to prevent electric shock or other dangers.
- If the device is not used for a long time, disconnect the power supply and unplug the power plug.
- If smoke, sound, or smell is emitted from the device, stop using the device immediately, disconnect the power supply, unplug the power plug and other cables, and remove the batteries. Then, contact the appointed maintenance center for repair.
- Ensure that no object (such as metal shavings) enters the device through the heat dissipation vent.
- Before connecting any other cable, connect the ground cable of the device. Do not disconnect the ground cable until you have disconnected all the other cables.
- Ensure that the three-phase power socket is grounded properly. The neutral line and the live line cannot be connected inversely.
- Do not scratch or abrade the shell of the device. The shed painting may lead to skin allergy or malfunction of the device. If the shed painting material drops into the host, a short circuit may occur.

Cleaning Precautions

- Before cleaning the device, stop using it, disconnect the power supply, and unplug all the cables connected to the device, including the power cable, telephone cable, video cable, audio cable, network cable, and serial cable.
- Do not clean the device shell with any cleaning solution or cleanser spray. Use a piece of soft cloth to clean the device shell.

Battery Usage Precautions of the Remote Control

- Use only the recommended battery. Pay attention to the polarity of the batteries while installing them.
- If a battery does not fit in the device, do not apply force. Otherwise, the battery may leak or explode.
- To reduce the risk of explosion, do not use batteries of different types together. For example, do not use an alkaline battery and a Mn-Zn battery together. It is recommended that you use batteries provided or recommended by the manufacturer.
- Do not use a new battery with an old battery. When you replace batteries, replace all of them at the same time.
- If you are not going to use the device for a long time, remove all the batteries.
- If any battery leaks, emits smoke, or emits abnormal smell, stop using it immediately.

- If the battery fluid comes in contact with your skin or clothes, rinse with water immediately and seek medical assistance.
- If the battery fluid goes into your eyes, do not rub your eyes. Rinse your eyes with water immediately and seek medical assistance.

Wireless Product Usage Precautions

- Keep the wireless device away from magnetic storage devices, such as a magnetic card or a floppy disk to prevent loss of the stored information.
- Stop using the wireless device and disconnect it from the power supply in places where using of wireless devices is prohibited or using of a wireless device may lead to interference or danger.
- Unplug the wireless device from the endpoint and turn off the endpoint close to a high-precision controlled electronic device, such as an audio phone, a pacemaker, fire alarm, or an automatic gate. Otherwise, this will lead to malfunction of the electronic device.
- The user who uses an electronic assistant medical-treatment device needs to confirm with the service center regarding the effects of the radio wave on this device.
- Do not take the wireless device to the operation theater, Intensive Care Unit (ICU), or the Coronary Care Unit (CCU).
- When using the device, ensure that the antenna of the device is at least 20 cm away from all parts of your body.
- In the area with inflammable or explosive materials, turn off your wireless device and follow the relevant instructions given on the label to prevent an explosion or fire.
- Use your wireless device and its accessories in a clean and dust-free environment. Ensure that the wireless device does not come in contact with flame or a lit cigarette.
- Ensure that the wireless device and its accessories are dry.
- Do not drop, throw, or bend your wireless device.
- Do not place the wireless device and its accessories in areas with extreme temperatures.

Environmental Protection

Do not dispose of the device in a garbage can. The device, packing materials, batteries, and any discarded components or units must be disposed of in accordance with local regulations in order to support recycling activities.

Statement on a Class A Product

This is a class A product. In a national environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Regulatory Compliance

The endpoint complies with the following European directives and regulations.

- 1999/5/EC (R&TTE)
- 2002/95/EC & 2011/65/EU (RoHS)
- EC NO. 1907/2006 (REACH)
- 2002/96/EC (WEEE)

The endpoint complies with Directive 2002/95/EC, 2011/65/EU and other similar regulations from the countries outside the European Union, on the RoHS in electrical and electronic equipment. The endpoint does not contain lead, mercury, cadmium, and hexavalent chromium and brominated flame retardants (Polybrominated Biphenyls (PBB) or Polybrominated Diphenyl Ethers (PBDE)) except for those exempted applications allowed by RoHS directive for technical reasons.

The endpoint complies with Regulation EC NO. 1907/2006 (REACH) and other similar regulations from the countries outside the European Union. Huawei will notify to the European Chemical Agency (ECHA) or the customer when necessary and regulation requires.

The endpoint complies with Directive 2002/96/EC on waste electrical and electronic equipment (WEEE). Huawei is responsible for recycling its end-of-life devices, and please contact Huawei local service center when recycling is required. Huawei strictly complies with the EU Waste Electrical and Electronic Equipment Directive (WEEE Directive) and electronic waste management regulations enacted by different countries worldwide. In addition, Huawei has established a system for recycling and reuse of electronic wastes, and it can provide service of dismantling and recycling for WEEE. By Huawei recycling system, the waste can be handled environmentally and the resource can be recycled and reused fully, which is also Huawei WEEE stratagem in the word. Most of the materials in the endpoint are recyclable, and our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

In accordance with Article 11(2) in Directive 2002/96/EC (WEEE), The endpoints were marked with the following symbol: a cross-out wheeled waste bin with a bar beneath as below:



North American Regulatory Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device does not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

If this device is modified without authorization from Huawei, the device may no longer comply with FCC requirements for Class A digital devices. In that a case, your right to use the device may be limited by FCC regulations. Moreover, you may be required to correct any interference to radio or television communications at your own expense.



CAUTION

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.



NOTICE

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the device is operated in a commercial environment.

This device generates, uses and radiates radio frequency energy. If it is not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

Operation of this device in a residential area is likely to cause harmful interference. In this case the user will be requested to correct the interference at his or her own expense.

This device complies with RSS-247 of Industry Canada. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference.
- (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class A digital apparatus complies with Canadian ICES-003.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage.
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet appareil numérique de classe A est conforme à la norme ICES-003 du Canada.

Cet équipement est conforme aux limites IC d'exposition aux radiations définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à distance minimum de 20cm entre le radiateur et votre corps.

E Glossary

Numerics

802.1X An access control and authentication protocol based on the client/server mode. It can prevent unauthorized users/equipment from accessing the LAN/WLAN through an access port. After a client (STA) is associated with an AP, the 802.1X authentication result determines whether the STA can use the wireless services provided by the AP. If the STA passes the authentication, the STA can access the resources in the WLAN. If the STA fails to pass the authentication, the STA cannot access the resources in the WLAN.

A

AAC advanced audio coding

AES See [Advanced Encryption Standard](#).

API See [application programming interface](#).

Advanced Encryption Standard (AES) A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). It supersedes the Data Encryption Standard (DES). AES adopts a symmetric-key algorithm for both encrypting and decrypting the data, where the block size is 128 bits and the key size is 128 bits, 192 bits, or 256 bits.

application programming interface (API) An application programming interface is a particular set of rules and specifications that are used for communication between software programs.

D

DES See [Data Encryption Standard](#).

DHCP See [Dynamic Host Configuration Protocol](#).

Data Encryption Standard (DES) A specification for encryption of computer data developed by IBM and adopted by the U.S. government as a standard in 1976. DES uses a 56-bit key.

Dynamic Host Configuration A client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting information the host requires

Protocol (DHCP) to participate on the Internet network. DHCP also provides a mechanism for allocating IP addresses to hosts.

F

FTP File Transfer Protocol

FTPS See [File Transfer Protocol over SSL](#).

File Transfer Protocol over SSL (FTPS) An extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

G

G.722 Audio codec standard that uses adaptive differential pulse-code modulation (ADPCM). Its data rate is 48 kbit/s, 56 kbit/s, or 64 kbit/s.

H

H.264 Compared with H.263, H.264 can provide the same-quality video at half of the bit rate, with strong error resilience characteristics.

HD high definition

HDMI high definition multimedia interface

HTTP See [Hypertext Transfer Protocol](#).

HTTPS See [Hypertext Transfer Protocol Secure](#).

Hypertext Transfer Protocol (HTTP) An application-layer protocol used for communications between web servers and browsers or other programs. HTTP adopts the request-response mode. A client sends a request to the server. The request consists of two parts: request header and MIME-like message. The request header contains request method, uniform resource locator (URL), and protocol version. The MIME-like message contains request modifiers, client information, and possible body content. Upon receiving the request, the server responds with a status line. The status line includes the message's protocol version, a success or error code, and a MIME-like message, which contains server information, entity meta-information, and possible entity-body content. For details about HTTP, see RFC2616.

Hypertext Transfer Protocol Secure (HTTPS) An HTTP protocol that runs on top of transport layer security (TLS) and Secure Sockets Layer (SSL). It is used to establish a reliable channel for encrypted communication and secure identification of a network web server. For details, see RFC2818.

I

IMS IP multimedia subsystem

| | |
|---|--|
| IPv4 | See Internet Protocol version 4 . |
| IPv6 | See Internet Protocol version 6 . |
| Internet Protocol version 4 (IPv4) | The current version of the Internet Protocol (IP). IPv4 utilizes a 32bit address which is assigned to hosts. An address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods and may range from 0.0.0.0 through to 255.255.255.255. Each IPv4 address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. |
| Internet Protocol version 6 (IPv6) | An update version of IPv4, which is designed by the Internet Engineering Task Force (IETF) and is also called IP Next Generation (IPng). It is a new version of the Internet Protocol. The difference between IPv6 and IPv4 is that an IPv4 address has 32 bits while an IPv6 address has 128 bits. |
| L | |
| LDAP | See Lightweight Directory Access Protocol . |
| Lightweight Directory Access Protocol (LDAP) | A network protocol based on TCP/IP, which allows access to a directory system agent (DSA). It involves some reduced functionality from X.500 Directory Access Protocol (DAP) specifications. |
| M | |
| MCU | See multipoint control unit . |
| multipoint control unit (MCU) | Data connection equipment used in a videoconferencing system. An MCU is used for terminal access, video exchange, audio mixing, data processing, and signaling exchange. |
| S | |
| SIP | Session Initiation Protocol |
| SNMP | See Simple Network Management Protocol . |
| SRTP | See Secure Real-time Transport Protocol . |
| SSID | See service set identifier . |
| Secure Real-time Transport Protocol (SRTP) | A real time transport protocol with enhanced security and encryption mechanism-based RTP. |
| Simple Network Management Protocol (SNMP) | A network management protocol of TCP/IP. It enables remote users to view and modify the management information of a network element. This protocol ensures the transmission of management information between any two points. The polling mechanism is adopted to provide basic function sets. According to SNMP, agents, which can be hardware as well as software, can monitor the activities of various devices on the network and report these activities to the network console workstation. |

Control information about each device is maintained by a management information block.

service set identifier (SSID) SSID can divide a wireless LAN into multiple subnets, and perform separate identity authentication on each subnet. Only the users passed the authentication can access the corresponding subnet.

T

TCP See [Transmission Control Protocol](#).

TCP/IP Transmission Control Protocol/Internet Protocol

TLS Transport Layer Security

Transmission Control Protocol (TCP) The protocol within TCP/IP that governs the breakup of data messages into packets to be sent using Internet Protocol (IP), and the reassembly and verification of the complete messages from packets received by IP. A connection-oriented, reliable protocol (reliable in the sense of ensuring error-free delivery), TCP corresponds to the transport layer in the ISO/OSI reference model.

V

VoIP See [Voice over Internet Protocol](#).

Voice over Internet Protocol (VoIP) A value-added service technology for IP calls. The VoIP service is a new IP telecom service. It can run on fixed and mobile networks and support flexible access points. Fees for VoIP subscribers are relatively low. Calls between VoIP subscribers who belong to the same carrier are free of charge.

W

WLAN See [wireless local area network](#).

WPA-PSK Wi-Fi protected access pre-shared key

wireless local area network (WLAN) A hybrid of the computer network and the wireless communication technology. It uses wireless multiple address channels as transmission media and carries out data interaction through electromagnetic wave to implement the functions of the traditional LAN.