

**Huawei SMC**  
**20.1.0**

# Product Overview

**Issue**            01  
**Date**             2020-03-31



**Copyright © Huawei Technologies Co., Ltd. 2020. 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**



HUAWEI 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: <https://e.huawei.com>

---

# Contents

---

<b>1 Product Positioning and Highlights.....</b>	<b>1</b>
1.1 Service Positioning.....	1
1.2 Highlights.....	3
<b>2 Application Scenarios.....</b>	<b>5</b>
2.1 CloudLink Edge 1000 Small-Scale Networking.....	5
2.2 SMC and MCU Medium- And Large-Scale Networking.....	6
2.3 Endpoint Extranet Access Networking.....	7
<b>3 Product Structure.....</b>	<b>9</b>
3.1 System Architecture.....	9
3.2 Installation and Deployment.....	11
<b>4 Features and Functions.....</b>	<b>12</b>
4.1 Flexible Permission Management.....	12
4.2 Unified Resource Scheduling.....	14
4.3 Device Management.....	16
4.3.1 SC.....	16
4.3.2 Corporate Directory.....	18
4.3.3 MCU.....	19
4.3.4 Endpoint Management.....	20
4.3.5 License Management.....	20
4.4 Meeting Management.....	21
4.4.1 Diverse Conference Convening Modes.....	21
4.4.2 Data Conference.....	21
4.4.3 Convenient Multi-Level Conference.....	23
4.4.4 Predefined Conference Templates.....	23
4.4.5 Conference Recording, VoD, and Live Streaming.....	24
4.4.6 Rich Meeting Control Functions.....	24
4.4.7 AI Services.....	27
<b>5 Reliability.....</b>	<b>30</b>
<b>6 Security.....</b>	<b>31</b>
<b>7 Openness.....</b>	<b>33</b>
<b>8 Operations and Maintenance.....</b>	<b>34</b>

---

8.1 Different WebUIs.....	34
8.2 Software Upgrade.....	35
8.3 Data Backup.....	36
8.4 Logs.....	36
8.5 Alarms.....	39
8.6 One-click Information Collection.....	39
8.7 Device Upgrade.....	40
8.8 Device Inspection.....	40
<b>9 Technical Specifications.....</b>	<b>41</b>
9.1 Performance Specifications.....	41
9.2 Standards and Protocols Compliance.....	43
<b>10 Acronyms.....</b>	<b>45</b>

# 1 Product Positioning and Highlights

---

The HUAWEI Service Management Center (SMC) is a next-generation video conferencing service management system that provides easy-to-use conference management and control, visualized O&M, as well as unified management and scheduling of video conferencing devices and media resources on the entire network. It uses a service-oriented architecture featuring high performance, large capacity, and auto scaling, meeting needs of video conferences at different scales.

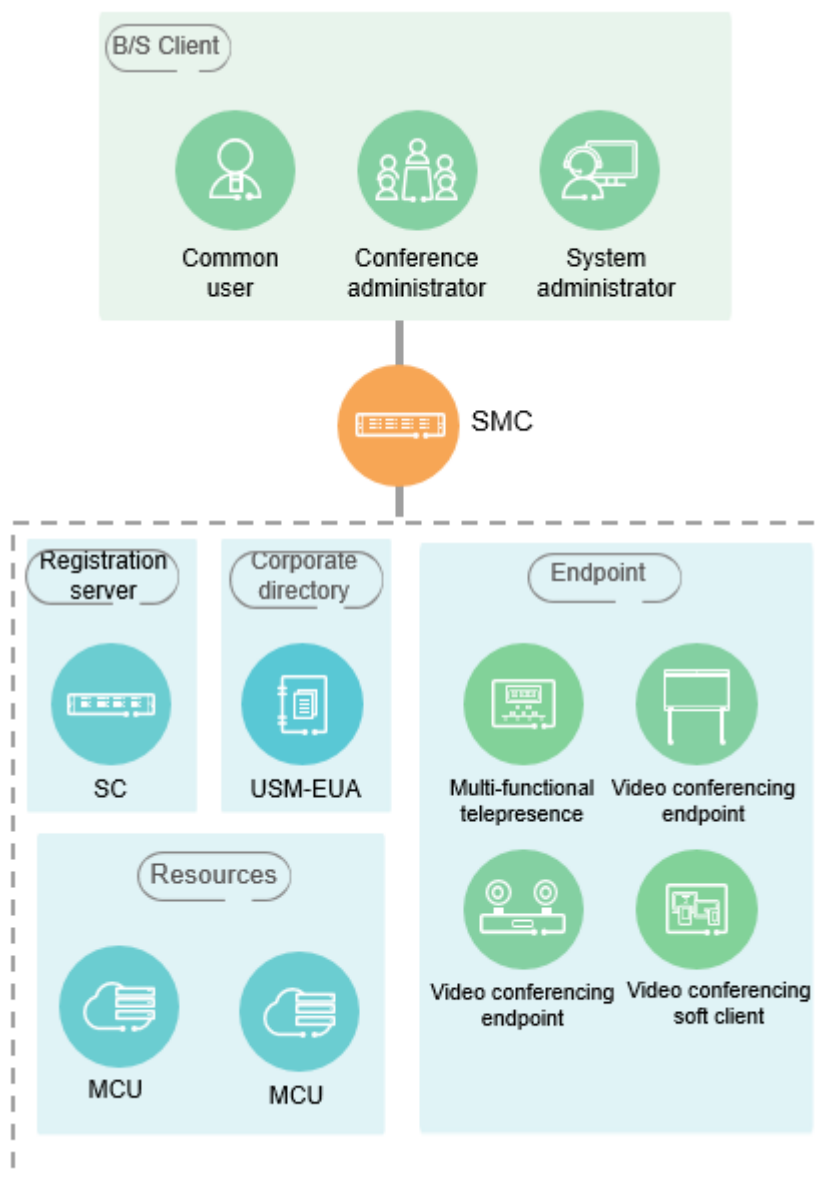
## 1.1 Service Positioning

This section describes the SMC positioning and its application in the basic networking. The SMC centrally manages and controls video conferencing devices and resources on the entire network, and offers a variety of conference scheduling modes. With flexible and comprehensive third-party APIs, the SMC easily integrates industry applications and interconnects with third-party systems, effectively improving communication and decision-making efficiency and greatly reducing O&M costs.

It offers unified management and centralized control, flexible and comprehensive third-party interfaces, as well as rich conference scheduling modes. With the mature video communications management system provided by the SMC, enterprise IT decision makers and users smoothly communicate and collaborate with each other, thereby greatly reducing enterprise operating expense.

**1.1 Service Positioning** shows the position of the SMC in the video conferencing service networking.

**Figure 1-1** Basic networking of the video conferencing service



With a cutting-edge architecture, the SMC provides the following features:

- **Ease of use:** The SMC comes with an intuitive web interface that allows users to interact with the video conferencing system easily and conveniently.
- **Intelligent management:** A unified management platform is used to manage devices and conferences based on user levels (system administrator, conference administrator, and common user).
- **Intelligent scheduling:** On a large or medium enterprise network, conference resources are intelligently allocated by service area to implement instant conference scheduling.

## 1.2 Highlights

Being capable of managing devices and meetings and compatible with a variety of third-party services and devices, the SMC is ideal for large video conferencing networks.

### **Relaxed Experience with Professional and Convenient Meeting Control**

- Personalized, custom meeting control functions: one-click roll call and broadcast, etc., enabling quick meeting control for enterprises and individuals
- Efficient meeting control: quick meeting locating by organization in a cascaded system, easy participant operations, and clear meeting and participant status
- Professional Visual Dispatching Center (VDC): audio and video pre-monitoring, presentation preview, custom combination of meeting controls, as well as live videos push to the video wall
- Quick initiation of large cascaded meetings: one-click scheduling using a meeting template or historical meeting, auto MCU cascading and management
- Integrated enterprise OA system: meeting scheduling or canceling via email client, viewing of status (free or busy) of participants and meeting rooms, and meeting notification emails automatically added to users' schedules

### **One-stop O&M with Unified Management of Network-wide Devices and Resources**

- Unified device management: centrally manage enterprise assets, including MCUs, recording and streaming devices, GK/SIP servers, corporate directories, telepresence systems, and endpoints
- Unified resource management: MCU resource pooling for intra- or inter-pool load balancing and backup, improving resource utilization and ensuring meeting continuity
- Unified management and configuration: auto configuration delivery, software management, status and performance management, and remote device diagnostics
- Easy O&M, real-time device status monitoring: batch parameter configuration and modification, software version management and batch upgrade, alarm query and handling, fault information export, remote device health check, and report generation
- Flexible, simplified statistical reports: video asset usage obtained in a timely manner, helping you adjust deployment and make decisions

### **Hierarchical and Role-based Management, Refined Permission Control**

- Hierarchical and role-based user management based on enterprise organizations, enabling flexible level definition and permission control
- Multi-role management: system administrators, meeting administrators, and common users are supported, offering device management, meeting management, and meeting scheduling by individual

## Flexible, Scalable Service-oriented Architecture

- Scenarios with less than 10,000 users: allowing the management platform to be deployed on a device, with built-in registration and call control, corporate directories, centralized deployment and management at the HQ, as well as MCU resource pool management supported. A single device supports 1000 concurrent calls.
- Scenarios with less than 200,000 users: allowing the management platform to be independently deployed on a large-capacity network, with distributed deployment and centralized management of MCUs for multi-level administrative meetings and enterprises with multiple branches supported. A single device supports 20,000 concurrent calls.
- RESTful APIs: supporting meeting management and control, as well as recording management, meeting the needs for integrating OA systems and industry applications.
- Connecting to mainstream monitoring platforms through VDC: enabling you to view monitored images and control cameras during a meeting, meeting industry application demands.



# 2 Application Scenarios

This section describes the use of the SMC in different application scenarios.

## 2.1 CloudLink Edge 1000 Small-Scale Networking

The CloudLink Edge 1000 is a small-sized video conferencing solution that supports 1000 users. One server integrates functions such as conference management, endpoint management, corporate directory, and media processing. It can connect to endpoints complying with various standard protocols, enabling flexible communication between internal and external branches and between employees.

**Figure 2-1** CloudLink Edge 1000 small-scale networking



In this networking scheme:

- High integration: Integrates functions including conference management, device management, media processing, corporate directory, call registration, and traversal between public and private networks.
- Flexible networking: A maximum of 500 concurrent calls and 1000 registered users are supported. MCUs and recording servers can be extended. Standalone SCs are supported in the extended DMZ scenario.

- Universal access: Supports voice and video as well as data conferences, and software and hardware terminal access.
- Rich and convenient user experience: Supports SiteCall, one-click conference joining, automatic video display, and multiple conference control functions.

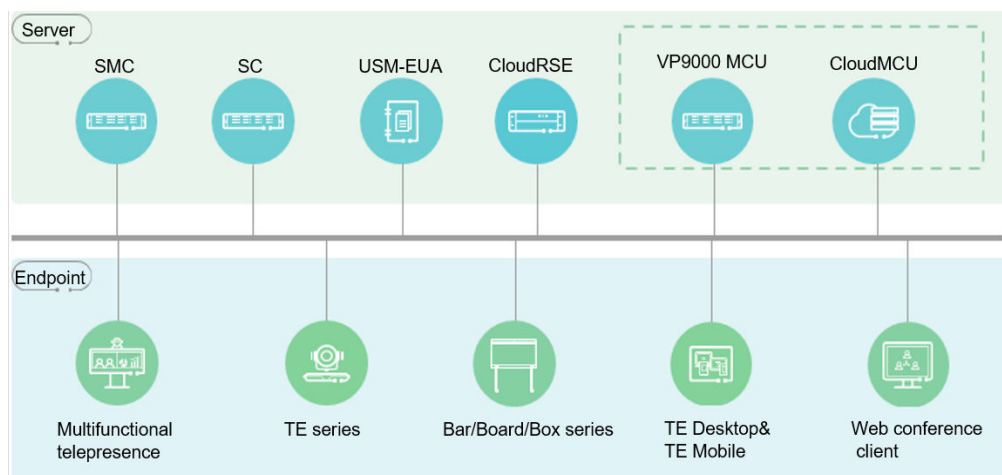
## 2.2 SMC and MCU Medium- And Large-Scale Networking

The video conferencing solution supports medium-scale scenarios with 10,000 users and large-scale scenarios with 200,000 users, meeting the requirements of different users.

**Figure 2-2** Medium- and large-scale networking principles



**Figure 2-3** Medium- and large-scale network planning



In this networking scheme:

- A medium-scale network supports a maximum of 1000 concurrent calls and 10,000 registered users. The service platform components SMC, SC, and USM-EUA are deployed on the same server.
- A large-scale network supports 20,000 concurrent calls and 200,000 registered users. The service platform components SMC and SC&USM-EUA are deployed on different servers.
- The VP9000 series MCU and CloudMCU can be deployed on the same network.

- Universal access: Supports voice and video as well as data conferences, and software and hardware terminal access.
- Rich and convenient user experience: Supports SiteCall, one-click conference joining, automatic video display, and multiple conference control functions.

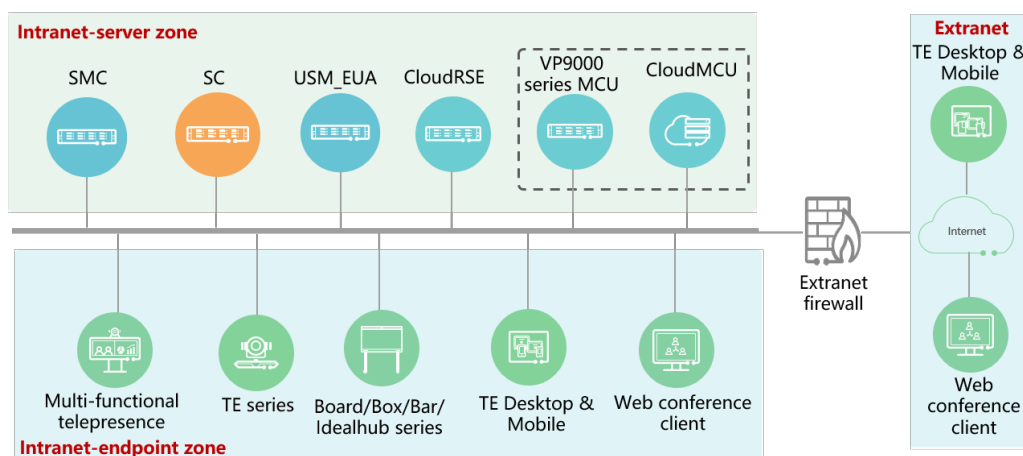
## 2.3 Endpoint Extranet Access Networking

To connect extranet endpoints and ensure network security, the intranet must be isolated from the Internet, with a firewall deployed at the network edge. The video conferencing solution provides different networking schemes based on different network scales and security requirements.

### Deployment in the Non-DMZ Scenario

By deploying the network that supports traversal between public and private networks with an intranet SC, you can implement audio and video communication between endpoints on the Internet and those on an enterprise intranet, which saves costs. [Figure 2-4](#) shows the networking.

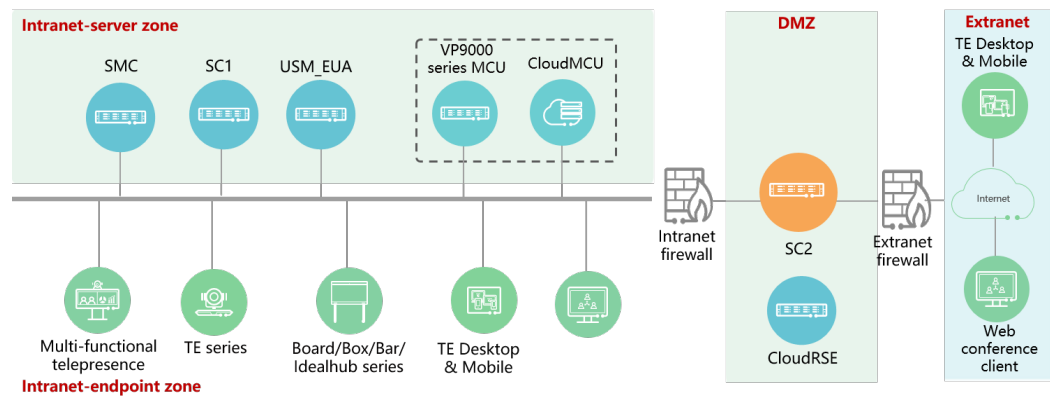
**Figure 2-4** Networking with an intranet SC



### Deployment in the DMZ Scenario

By deploying the network that supports traversal between public and private networks with a standalone SC in the DMZ, you can implement audio and video communication between endpoints on the Internet and those on an enterprise intranet, which achieves large-capacity deployment and high reliability. [Figure 2-5](#) shows the networking.

**Figure 2-5** Networking with SC deployed in the intranet and DMZ



# 3 Product Structure

---

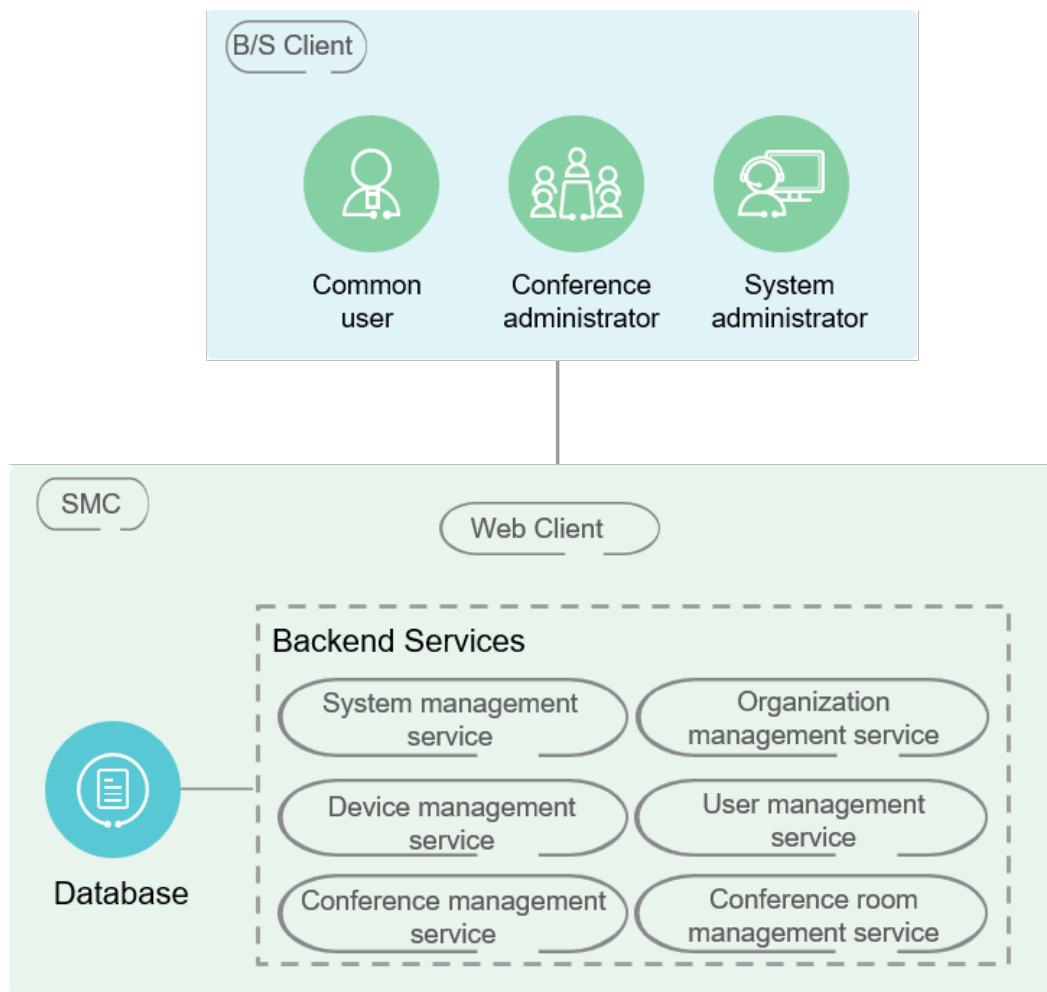
This section describes the system structure and appearance of the SMC, helping you have a better understanding of SMC.

## 3.1 System Architecture

The section describes the system structure of the SMC.

The SMC consists of three parts: the web client, back-end service, and database, as shown in [Figure 3-1](#).

**Figure 3-1** System architecture



The function of each part is as follows:

- **Web client**  
Provides man-machine interaction interfaces through which different types of users can perform operations on the SMC. System administrators can log in to the SMC to manage devices and set resource use policies. Meeting administrators can log in to the system and manage meetings under their own organizations. Common users are able to log in to the system to view the meeting room list and meeting templates under their organizations and schedule meetings.
- **Back-end service**  
Serves as the engine of the SMC and provides multiple meeting system services. The backend receives user requests returned by the web client and forwards these requests to each backend subservice by service module where each request belongs, implementing precise service provision and swift response.
- **Database**  
Works as the storage module to store SMC data. The data storage module of the SMC stores and reads a large amount of data during service system

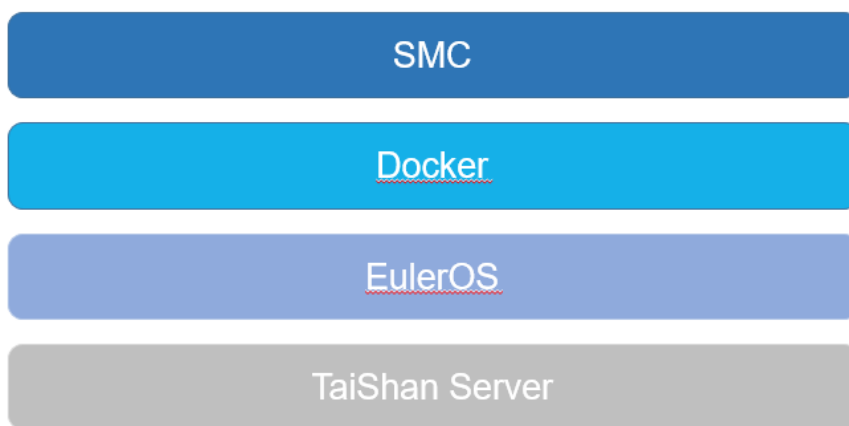
running. Efficient and stable data access ensures the SMC running stability and efficiency.

## 3.2 Installation and Deployment

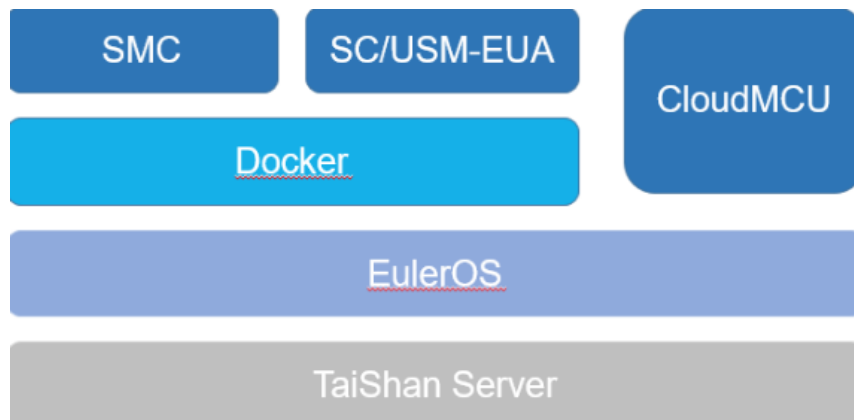
This section describes the SMC installation and deployment modes.

The SMC can be deployed in a single-node system on the TaiShan server using a software package. It can be deployed alone on a server or co-deployed with other NEs. [Figure 3-2](#) and [Figure 3-3](#) show how the SMC service is deployed on a TaiShan server.

**Figure 3-2** SMC service deployment (standalone deployment)



**Figure 3-3** Service deployment (co-deployed with other NEs)



# 4 Features and Functions

---

This section describes the main features and functions of the SMC.

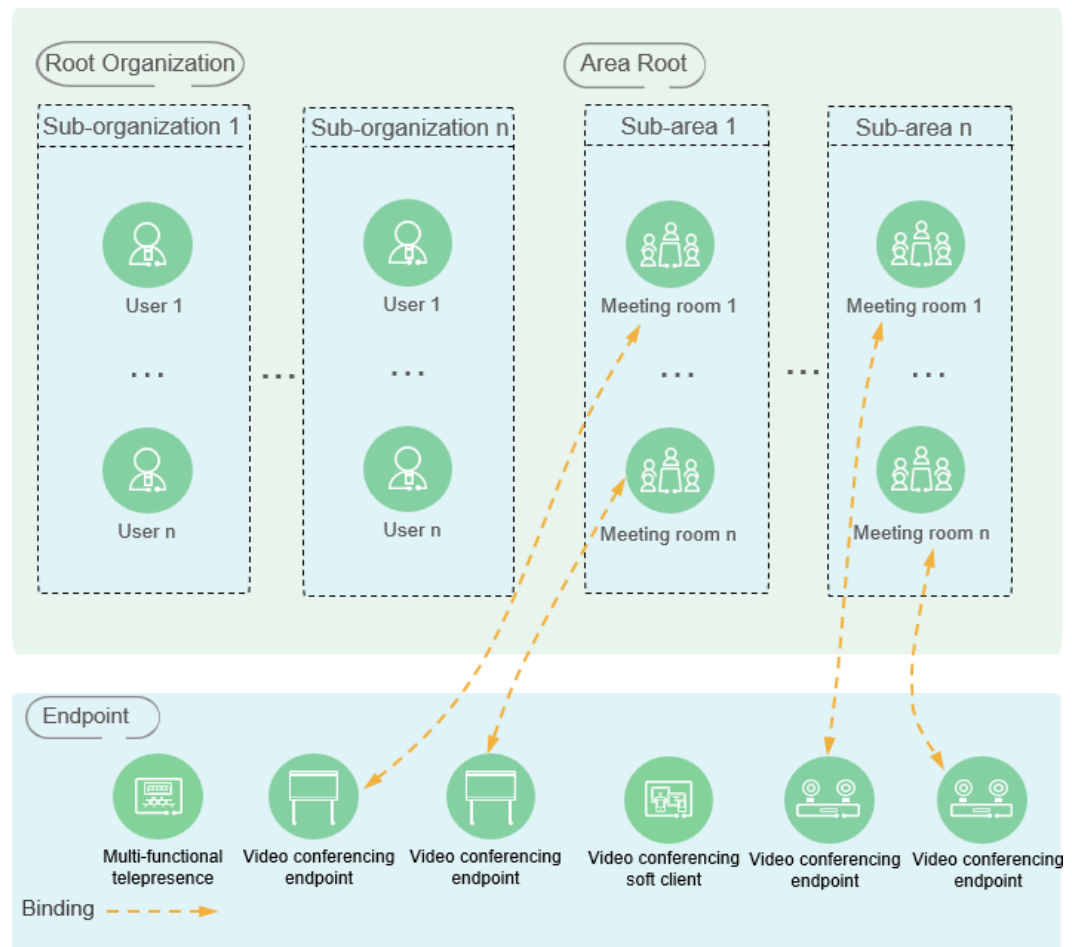
## 4.1 Flexible Permission Management

The rights-based management system of the SMC consists of organizations, areas, meeting rooms, and users. To provision a meeting room, you can set it to belong an area or an organization; to provision a user, a belonged organization must be selected. In this way, the structure and rights of meeting rooms and users are managed.

**Figure 4-1** shows the SMC service structure when meeting rooms belong to areas.



**Figure 4-1** Architecture



**Organization:** similar to a department. Users are managed based on the organization structure. When the SMC provisions meeting users, each user belongs to an organization.

**Area:** planned based on site requirements. You can select an area where the meeting room to be provisioned belongs.

**Meeting Room:** provisioned by the SMC. Each meeting room is bound to an endpoint that is used to join a meeting. Specifically, if a meeting room is invited to join the meeting, it is the endpoint in this meeting room that joins the meeting. When provisioning a meeting room, you can make it to share the organization tree with users or select a belonged area for it.

**User:** has three levels, including system administrator, meeting administrator, and common user. Default permissions cannot be modified or deleted. Meeting administrators and common users can choose whether to bind endpoints as needed. Users who have bound endpoints can use a corresponding endpoint to join conferences on the SMC.

- **System administrator:** has system management permissions authorized by the SMC, including device (endpoints, MCUs, SCs, as well as recording and streaming servers) management and system configuration. A system administrator cannot initiate or join a meeting, and does not belong to any organization.

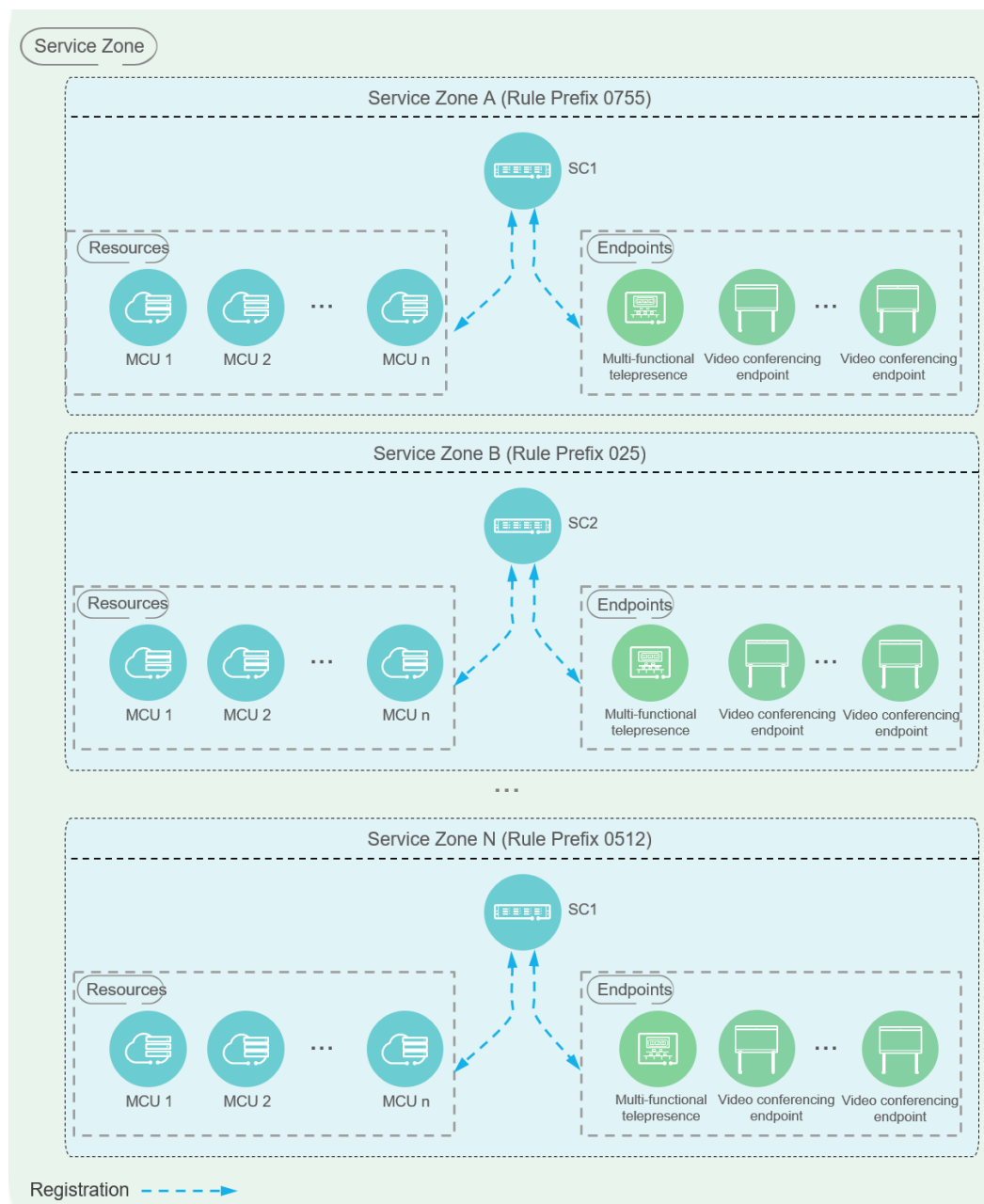
- Meeting administrator: can manage and operate meetings under the organization and its sub-organizations.
- Common user: can operate conferences under the organization and its sub-organizations, such as creating meetings (instant, scheduled, or recurring conferences), creating meetings using templates, viewing scheduled and historical meetings, as well as configuring meeting policies and capabilities.

## 4.2 Unified Resource Scheduling

The SMC can manage the resources that are distributed by using multiple service areas.

During conference scheduling, endpoints in a service area preferentially use resources that match the service area prefix to optimize resource configuration and use at the service area level. [Figure 4-2](#) shows the SMC service area architecture.

Figure 4-2 Service area architecture



- The SMC can divide a network into multiple service areas by area. Users are able to configure matching rules for each service area, and modify or delete service areas.
- One service area can have only one registered SC and one extranet SC, while one SC can belong to multiple service areas. If no SC is specified for a service area, endpoint numbers provisioned to the service area will not be delivered to the SC.
- An MCU can be registered with SCs in only one service area. Users can modify the service area where the MCU belongs.
- An endpoint can register with SCs in only one service area. (The system administrator binds an endpoint and configures the registration number when

adding a conference room or user. The number prefix needs to match the service area rules.) Users can change the belonged service area by changing the registration number.

## 4.3 Device Management

The SMC manages the access of devices such as SCs, USM-EUA, MCUs, and endpoints, and provides a web interface for users to configure and maintain these devices.

### 4.3.1 SC

The Switch Center (SC) is a registration and call control server that can be used to implement seamless video communication between the intranet and extranet, between the headquarters and branches, and between enterprises.

The SMC provides the SC with a web interface on which system administrators can directly operate SC, such as delivering key configurations, monitoring the status, and maintaining the SC. [Table 4-1](#) describes the parameters.

**Table 4-1** SC management

Configuration Item	Description
Basic Information	Specifies the SC authentication settings. System administrators can configure, view, and modify these settings.
Parameters	Specifies all key configurations of the SC. System administrators can view and modify these configurations.
Area Management	<p>An area is a geographically or virtually defined unit. SC services are implemented by area.</p> <p>Areas are classified into local and neighboring areas.</p> <ul style="list-style-type: none"><li>• Local area: an area that is created to restrict communication of nodes (including endpoints, MCUs, and gateways) registered with the local SC.</li><li>• Neighboring area: an area that is created to restrict communication of nodes (including endpoints, MCUs, and gateways) registered with a remote SC.</li></ul> <p>After areas are created, the following video conferencing services can be managed by area: node registration, node calling, bandwidth allocation, and call bandwidth control.</p>
Registration List	Specifies the information in relation to all devices registered with the SC, including the alias, address, device information, protocol in use, call records, and alias list.
Log	Specifies the SC operation logs that you can view and export.

Configuration Item	Description
Signaling Diagnosis	Allows you to diagnose and export real-time calls and registration signaling of the SC.
Alarms	Specifies the alarms generated during the SC running, which can be viewed and cleared.
Member Rule	Specifies member rules that are used to define the policy for determining the number, URI, node alias, and IP address. These policies determine the area where a registered device belongs. After adding a member rule, the area where a device belongs can be determined.
Local Management Domain	By configuring one or more local management domains for each SC, the management scope of each SC is specified.
Called Number Change	During a call, if a called number matches a specified alias based on the rule, the called number is changed. Users can use this process when they want to hide their real numbers.
Calling Number Change	During a call, if a calling number matches a specified alias based on the rule, the calling number is changed. In this case, the function is used to avoid the following scenario: a terminal number must be unique, and a calling number can access only one conference.
Search Rule	A search rule helps the SC identify the area where a called party belongs.
Call List	On the <b>Call List</b> tab page, you can view and release calls between devices registered with the SC. The call list page records the start time of a call, alias of the calling/called device, protocol used by the calling/called device, bandwidths allocated by the system, and specifies whether a soft client request a license from the SMC when initiating a call.
Bandwidth Management	The SC uses bandwidth management to flexibly restrict the bandwidths of calls between two specified areas. With this function, audio/video quality degradation can be avoided if the cross-area call traffic is too large. If a bandwidth rule is configured between two areas, the SC will check the call when devices in the two areas call each other. If the call does not meet the bandwidth rule, the SC will release the call or reduce the call rate.

Configuration Item	Description
Route Restriction	<p>The route restriction function of the SC enables two nodes that cannot communicate with each other to implement media (audio and video) communication under the SC forwarding.</p> <p>If two nodes registered with the same SC belong to different areas and media communication between these two areas is unavailable due to network disconnection or firewall restrictions, all calls between these two areas are forwarded by the SC for media communication if route restrictions are configured.</p>
Predefined Nodes	<p>If a device fails to be added on the SMC, go to the predefined node list and add or delete the number allocation information of the device or add the authentication information for the device that does not need to be managed by the SMC but needs to register with the SC.</p>
Certificate Management	<p>On the SMC web interface, you can import or delete SC certificates.</p>
Reverse Proxy	<p>The SC supports the NATP/HTTP reverse and web data service proxies to implement functions such as corporate directory access from intranet and extranet endpoints, SiteCall, and data conference sharing.</p>

### 4.3.2 Corporate Directory

The CloudUSM-EUA (USM-EUA for short) is deployed to synchronize information between the SMC and USM-EUA. In this way, users can select meeting rooms or users from the USM-EUA when holding meetings on the SMC.

The USM-EUA provides corporate directory services based on the LDAP protocol and is managed by the SMC.

The SMC can synchronize the following information to the USM-EUA:

- Area structure information: The information about adding, deleting, or modifying areas is synchronized to the USM-EUA.
- Conference room information: Information about adding or deleting a conference room, modifying the conference room organization relationship, or modifying some conference room parameters is synchronized to the USM-EUA.
- User information: Information about adding, deleting, or modifying conference administrators or common users is synchronized to the USM-EUA.

On the SMC web interface, you can manage the USM-EUA. Specifically, with the SMC, a system administrator can deliver key configurations to the USM-EUA and operate or maintain the USM-EUA. [Table 4-2](#) describes the parameters.

**Table 4-2** USM-EUA management

Configuration Item	Description
Basic Information	Specifies the interconnection information between the SMC and USM-EUA. System administrators can configure, view, or modify the information.
Service Address	Due to the differences in the endpoint network deployment, configure multiple service addresses for connecting to the USM-EUA based on the network plan. Multiple service IP addresses can be configured for the USM-EUA on the SMC.
3rd-LDAP Synchronization	The USM-EUA can interwork with a third-party LDAP server to implement directory communication.
Permission Control	System administrators can configure whether to control the query permission of users and whether to allow all users to access the organization structure directory.
Other Settings	These settings include security level, sorting, node name, and projection code. <ul style="list-style-type: none"><li>• Security level for accessing the corporate directory: System administrators can configure the security level for accessing the USM-EUA based on network requirements.</li><li>• Sorting information about the enterprise address book: including the sorting rule, sorting mode, and sorting field</li><li>• Node name of the corporate directory: System administrators can change node names as needed.</li><li>• Wireless projection code: The USM-EUA generates wireless projection code ranges for endpoints. System administrators can configure the ranges as needed.</li></ul>
Configure AI	The USM-EUA can connect to the facial recognition server for facial recognition sign-in and on-screen name tag functions.
Alarms	Specifies the alarms generated during USM-EUA running that users can view and clear.
Log	You can view and export USM-EUA operation logs on the log tab page.

### 4.3.3 MCU

MCUs and recording and streaming servers are used as resources on the SMC. The SMC adopts different policies for scheduling these resources.

The SMC allows you to manage and schedule MCUs as follows:

- On the SMC web interface, you can add, modify, and delete MCUs.
- On the SMC web interface, you can view the MCU details, alarms, logs, membership, usage, etc.
- The SMC centrally manages and schedules MCUs to implement load balancing, sharing, and redundancy backup of MCU resources.

The SMC supports the following types of MCUs:

- CloudMCU: a software-based conference server. The CloudMCU forwards video streams in multiple resolutions from only a single endpoint. After receiving multiple streams, the endpoint combines them into continuous presence without additional transcoding, improving user experience.
- VP9000 series MCU: The default initial resource type is universal transcoding. A universal transcoding MCU allows endpoints with any protocol, format, or bandwidth to join a meeting, with port resources flexibly allocated.

### 4.3.4 Endpoint Management

The SMC provides a unified endpoint management system that allows you to activate manageable endpoints using activation codes. Additionally, you can deliver configurations to endpoints in batches, as well as manage endpoint alarms and logs.

With this system, you can:

- Connect a manageable endpoint with the SMC using an activation code. After the activation is successful, the SMC delivers the SC, USM-EUA, and endpoint registration accounts to the endpoint. The endpoint then automatically registers with the SMC.
- Add a configuration file for a manageable endpoint. After the endpoint is activated, you can deploy a configuration task to deliver the time and language information to the endpoint.
- Filter endpoints by IP address segment, device model, and SN, and manage user-defined groups.
- Upload the version file of the endpoint. Additionally, you can upgrade one or more endpoints using an upgrade task.
- Upload endpoint certificates on the SMC. You can centrally deliver certificates to endpoints for certificate application by using a certificate deployment task.
- Collect and export endpoint logs. An endpoint automatically reports its logs to the SMC.
- View and handle the alarms on the SMC. An endpoint can report alarms to the SMC.

### 4.3.5 License Management

The SMC provides a floating license to centrally manage SCs, MCUs, as well as recording and streaming servers, facilitating resource control.

The license controls the following items:

- SMC and SC encryption disabling
- Floating traversal traffic



- Number of convergent video channels
- Number of concurrent conference ports
- Concurrent authorization for third-party advanced users
- Number of registered soft clients and conference terminals
- Number of registered devices and managed devices
- Number of video recording ports and live streaming ports

On the SMC, you can:

- Import a license: After a user imports a license issued by Huawei, the user can use the resources authorized by the license after the license takes effect. An imported new license will overwrite the old license.
- Revoke a license: After a license is revoked, it enters a 60-day grace period. Sixty days later, the license turns to the default state.
- View license resources: Users can view license resource control information.

## 4.4 Meeting Management

Conferences on the SMC involve two parts: 1) adapt conference parameters, schedule resources, and manage relationships between conference instances and nodes; 2) manage conferences, including active and scheduled conferences, and control conferences.

### 4.4.1 Diverse Conference Convening Modes

The video conferencing solution allows users to convene conferences in diverse and flexible ways.

- Initiate a conference from the SMC web interface using a conference template or by creating a new conference.
- Use the SiteCall function of an endpoint to create a conference.
- Use a third-party interface to convene a conference.
- Use the Outlook to convene a conference.

### 4.4.2 Data Conference

The video conferencing solution provides the data conference service based on VP9800 series MCUs or the CloudMCU. During conferences, users can use functions such as desktop sharing, whiteboard, document sharing, file transfer, text communication, and questionnaire survey to achieve efficient communication and collaboration.

The video conferencing solution supports 4K and 1080p60 HD data conference resolutions. Users can select a proper HD resolution based on their network bandwidth and terminals to enjoy HD data conference experience. Currently, only RoomPresence series, IdeaHub Pro/S, and Bar/Board/Box series support the 4K encoding in desktop sharing. The total call bandwidth must be 2 Mbit/s or higher.

## Data Collaboration

[Table 4-3](#) lists data collaboration functions for different roles in a conference.

**Table 4-3** Data collaboration functions

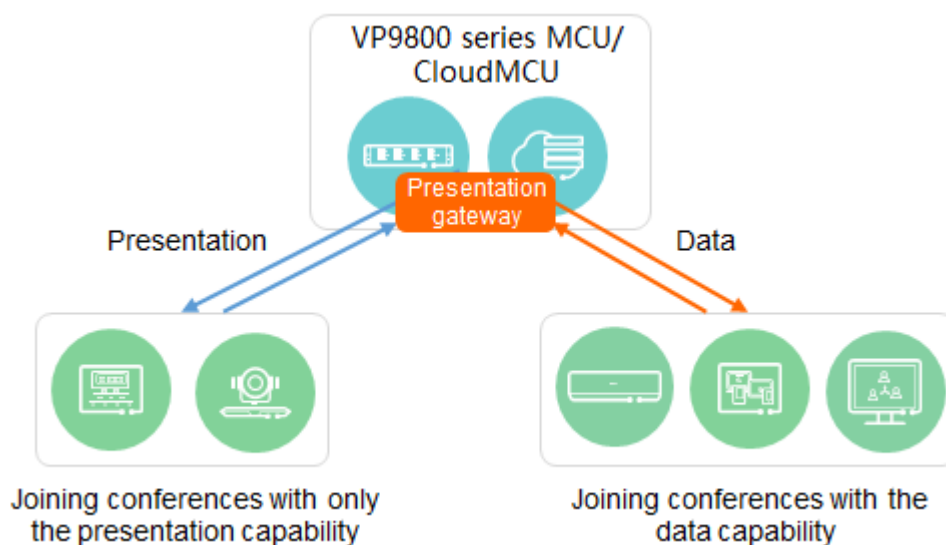
Role	Function
Chair	<ul style="list-style-type: none"><li>• Viewing participant video</li><li>• Broadcasting participant video</li><li>• Transferring to another number</li><li>• Sending a conference IM</li><li>• Sharing a document</li><li>• Taking notes, recording a conference, releasing a bulletin, and transferring a file</li></ul>
Presenter	<ul style="list-style-type: none"><li>• Viewing participant video</li><li>• Transferring to another number</li><li>• Sending a conference IM</li><li>• Performing data collaboration operations, such as document sharing, whiteboard, desktop, program, and media</li><li>• Inviting a participant to share the desktop</li><li>• Taking notes, recording a conference, releasing a bulletin, and transferring a file</li><li>• Initiating a poll</li></ul>
Participant	<ul style="list-style-type: none"><li>• Viewing participant video</li><li>• Transferring to another number</li><li>• Sending a conference IM</li><li>• Taking notes</li></ul>

## Interoperability Between Presentations and Data

The presentation gateway of the VP9800 series MCU/CloudMCU enables interoperability between presentations and data.

- Users can access data conferences using the Web Client, TE Desktop/TE Mobile, RoomPresence series, IdeaHub Pro/S, and Bar/Board/Box series. The VP9800 series MCU/CloudMCU and the preceding terminals support data sharing encoding and decoding to implement data conference functions.
- Traditional video conferencing endpoints, such as the RP100, RP200, TP series, and TE series endpoints, do not support data sharing encoding and decoding. These endpoints can use interoperability between presentations and data to join data conferences that support various types of endpoints.

**Figure 4-3** Interoperability between presentations and data



### 4.4.3 Convenient Multi-Level Conference

On the SMC, common conferences can be cascaded to form a multi-level conference in a specified structure.

#### Typical Scenario 1

A provincial seminar that contains conference centers in both cities A and B needs to be held. Typically, conference templates A and B are respectively used to initiate conferences for conference centers in cities A and B. In this case, conference templates A and B can be merged to form a multi-level conference template. Using this multi-level conference template, conference centers in both cities A and B can join the seminar together, without the need to redefine conference templates of cities A and B.

#### Typical Scenario 2

Conference center A is holding a food seminar, while conference center B is holding a healthy life seminar. To merge these two seminars, multi-level conferencing can be used.

### 4.4.4 Predefined Conference Templates

A conference template is a collection of conference parameter settings that are stored in the SMC, including the conference participants. With a template, you can schedule conference at any time, improving conference initiation efficiency.

The following four types of conferences can be held on the SMC using a template:

- Instant conference: A conference is held immediately based on the template. You can set the conference duration to permanent, that is, the conference is always ongoing.
- One-time conference: A conference is scheduled and starts at the specified point in time. The conference is held only once.

- **Recurring conference:** A conference is held daily, weekly, or monthly. When the specified period arrives, the conference is automatically held.
- **Multi-level conference:** A cascaded conference is held quickly based on the levels specified in a multi-level conference template.

## 4.4.5 Conference Recording, VoD, and Live Streaming

The CloudRSE supports single-stream and multi-stream recording in a multipoint video conferencing network and allows users to play live broadcast and VOD on the web.

### Multipoint Recording

- **Recording and Streaming Control**  
During conference recording, the conference administrator can control recording operations on the SMC, including pausing, resuming, or stopping recording. The conference recording status can also be viewed in real time on the CloudRSE web interface.  
The CloudRSE automatically records content by segment when the recorded file reaches a specified size.
- **Audio IVR Prompt**  
During a conference, the MCU prompts IVR messages for starting or pausing recording. Users can also customize IVR prompts so that they can learn about the recording status in real time. During the recording, the latest recording status icon is displayed on the video conferencing endpoint interface.

### Live Streaming and VOD via Web














- **Multiple Display Layouts**  
The CloudRSE enables videos and conference content to be displayed in layouts such as full-screen and Picture in Picture (PiP), meeting diversified video experience requirements.
- **Multiple Platforms, Free of Plug-ins**
  - Allows users to watch conference live video and VOD using their PCs, laptops, tablets, and smartphones.
  - Users can visit the CloudRSE web interface using mainstream browsers to view conference videos smoothly without installing additional plug-ins.


## 4.4.6 Rich Meeting Control Functions

On the SMC, meetings can be controlled centrally or separately. Users can search meetings and view their details, as well as operate active meetings using various meeting control functions provided by the SMC.

With icons on the meeting control menu bar, you can perform overall meeting control.










**Table 4-4** Meeting control icons on the top of the web interface





Icon	Description
 Invite Participant	Invites a meeting room that is not in a meeting or a temporary meeting room to join the meeting.
 Call Absent Participant	Invites the meeting room again if it does not join a meeting upon receiving an invitation.
 Mute All	Mutes or unmutes the microphones of all meeting rooms.
 Give the Floor	(For chair) Gives the floor to a meeting room. After this operation, the microphones of the other meeting rooms are muted, and the site that were given the floor displays the video automatically.
 Free Discussion	Unmutes the microphones and speakers of all meeting rooms and stops broadcasting the current meeting room.
 Set Continuous Presence	Sets continuous presence and the video source displayed in each pane.
 Enable Voice Activation	Specifies whether to use voice activation to switch the broadcasting participant during a meeting.
 Mute All Speakers	Mutes the microphones of all meeting rooms.
 Banner	Sets a banner displayed to all participants in a meeting.
 Captions	Sets captions displayed to all participants in a meeting.
 Lock Sharing	Locks the presentation shared by a participant.
 Extend Meeting	Extends the duration of a meeting.
 Start Recording	Records or stops recording the current meeting.

Icon	Description
 Tracking Mode	In tracking mode, only a meeting chair or administrator can control meetings. Other terminals can only request chair control rights and the floor.

In the meeting room list on the bottom of the web interface, right-click a meeting room and use the shortcut menu to control the meeting.

**Table 4-5** Meeting control icons on the bottom of the web interface

Icon	Description
 Broadcast	Enables other meeting rooms to view the video of the current meeting room.
 Give the Floor	Enables the other meeting rooms to view the video of the current meeting room and mutes the microphones of those meeting rooms.
 Set as Chair/Remove Chair Control	Sets or revokes chair control.
 Share Content/Cancel Sharing	Shares the meeting room or stops local content sharing.
 Lock Participant Sharing	After you lock the participant sharing in a meeting room, the other meeting rooms cannot share content. Only the meeting administrator can select a meeting room from the SMC to share content.
 View Participant	Sets the video source to be viewed in a meeting room.
 Lock Video Source	After the video source of a meeting room is locked, the video source that is being viewed is retained in the meeting room. In this way, the video being viewed is always displayed even if other operations such as broadcasting and giving the floor are performed.
 Mute/Unmute Microphone	Mutes or unmutes the microphone in a meeting room.
 Mute/Unmute Speaker	Mutes or unmutes the speaker in a meeting room.

Icon	Description
 Set as Favorite Site	If there are a large number of participants in a meeting, you can set some of them as favorite ones. You can click the <b>Favorite Site</b> tab above the meeting room list to quickly locate the participants you want and perform meeting control operations.
 Disconnect Participant	Disconnects the meeting room from the meeting, but the meeting room is still displayed in the participant list.
 Delete Participant	Disconnects a meeting room from the meeting and deletes the meeting room from the participant list.
 View Participant Details	Views the detailed information, real-time protocol, bandwidth, and capability of the participant.

## 4.4.7 AI Services

The video conferencing solution applies AI technologies in the conference system to provide capabilities such as voice recognition and facial recognition, improving conference experience and work efficiency.

AI services, including voice commands, facial recognition sign-in, and on-screen name tag, are mainly implemented through RoomPresence series, IdeaHub Pro/S, and Bar/Board/Box series endpoints. The voice command service is only supported by RoomPresence 65T, Bar 500, Board, and Box 500/700/900.

### Voice Commands

You can say "Hey, Scotty" to the connected microphone to wake up "Scotty", the intelligent voice assistant, and then operate the endpoint using voice commands.

For example, after the intelligent voice assistant on HUAWEI Board wakes up, you will see the screen shown in [Figure 4-4](#).

**Figure 4-4** Intelligent voice assistant wakes up



You can then perform the following operations using voice commands:

- Initiating or canceling a call
- Creating a conference
- Joining a scheduled conference
- Extending a conference
- Adding participants to a conference
- Viewing participants or continuous presence
- Sharing or stopping content sharing over a cable
- Opening the whiteboard
- Adjusting the speaker volume at your site
- Muting or unmuting the microphones of other sites
- Starting intelligent diagnostics

## Facial Recognition Sign-In

In a conference that requires sign-in, the endpoint can automatically record sign-in information of users through facial recognition.

When scheduling a conference on the SMC, a user can specify whether the conference requires sign-in. If the user selects sign-in, sign-in is required in the conference. When participants arrive at the conference site at the sign-in time, use an endpoint to recognize participants' face information for sign-in. The user can view face sign-in details on the endpoint screen. After the conference ends, the SMC will send the conference sign-in result to the user's email box.



**Figure 4-5** Facial recognition sign-in



## On-Screen Name Tag

After the facial recognition function is enabled, the endpoint performs face detection in tracking mode during a conference. When a new face is detected and correctly matched on the facial recognition server, the server returns a name accordingly and adds the name tag to the face image. In this way, participants can view each other's name tag so that they can know each other.

**Figure 4-6** On-screen name tag



# 5 Reliability

---

The SMC adopts multiple backup mechanisms to ensure service continuity when any single device is faulty.

This highly-reliable design ensures the stable running of conferences and systems.

- **Resource Pool Backup**  
The SMC supports backup of MCU and recording and streaming server resource pools. If the MCU or recording and streaming server that holds a meeting is faulty, the SMC automatically switches the meeting to another available MCU or recording and streaming server in the same or standby service area. This ensures meeting continuity.
- **Service Area Backup**  
The SMC allows you to specify a standby service area for a service area. Specifically, if resources of the MCU or recording and streaming server (in the active service area) that holds the meeting are insufficient, the SMC automatically adds the meeting rooms that are not scheduled in the active service area to the standby one, ensuring meeting continuity.
- **Auto Recalling upon Abnormal Offline**  
If an IP-based endpoint goes offline abnormally during a conference, the SMC automatically invites the offline endpoint to join the conference again.
- **Communication Link Reconnection**  
After the SMC is disconnected from the MCU or recording and streaming server, the SMC can connect to them again and synchronize data.
- **Data Backup**  
The SMC allows you to manually back up the current system configuration and service data. The backup data can be used to restore SMC data if necessary.

# 6 Security

---

The SMC takes security measures at the application, system, network, and management layers, better securing user services.

## Application Layer

At the application layer, the security solution protects SMC applications using the following measures:

- Uses the PBKDF2, an authentication method, to ensure the security of the user login password.
- If a user enters an incorrect password for three consecutive times, a graphical verification code is required for the fourth login attempt. By default, after entering an incorrect password for five consecutive times, the user is locked out and must be unlocked by an administrator with higher permissions.
- Prompts users to change their passwords after the administrator resets the passwords.
- Enforces password complexity.
- Uses PBKDF2 to encrypt passwords before saving them to the database.
- Provides HTTPS for enhanced data transmission security. The SMC forcibly uses HTTPS for functions with high security requirements. For example, HTTPS is used during password change to prevent the current and new passwords from being transmitted in plaintext.
- Provides comprehensive logging to record and track user operations.

## System Layer

The security solution at the system layer protects the operating system and databases using the following measures:

- Provides security hardening policy files to harden operating system services and restrict operating system file permissions and account passwords, ensuring system access security.
- Provides security hardening policy files to harden databases and restrict database access, ensuring database access security.

## Network Layer

- Implements security on routers and switches, ensuring transmission security for the SMC database.
- Uses firewalls for security check, preventing the SMC from being attacked by malware.

## Management Layer

The security solution at the management layer implements logging and patch installation to ensure that the SMC runs properly.

# 7 Openness

---

The SMC provides third-party APIs for third-party developers to operate video conferences on the SMC such as querying and controlling video conferences.

It also offers RESTful APIs and Stomp-based subscription framework for third-party systems to integrate, customize, or perform secondary development. The SMC provides the following functions:

- Conference scheduling, scheduling, and control
- Simultaneous access of multiple accounts
- Encrypted HTTPS transmission

# 8 Operations and Maintenance

This section describes how to operate and maintain the SMC.

## 8.1 Different WebUIs

The SMC offers web interfaces for system administrators, meeting administrators, and common users.

**Table 8-1** describes the functions of the SMC web interface and related user roles and permissions.

**Table 8-1** Functions on the SMC web interface

Function	Description	System Administrator Portal	Meeting Administrator Portal	Common User Portal
Service Provisioning	You can manage meeting rooms and users on the SMC. Specifically, organizations, areas, users, meeting rooms, and roles can be managed.	√	x	x
Devices	You can manage MCUs, recording and streaming servers, SCs, corporate directory servers, endpoints, endpoint deployment, and deployment tasks.	√	x	x
System	You can manage SMC system parameters, including basic settings, security, email, meetings, AI, alarms, cloud-based collaboration, and quick deployment configuration.	√	x	x

Function	Description	System Administrator Portal	Meeting Administrator Portal	Common User Portal
Maintenance	You can manage SMC system maintenance items, including alarms, logs, licenses, certificates, database keys, device inspection, information collection, system upgrade, backup and restoration, and bulletin setting.	√	x	x
Create Meeting	Create a meeting.	x	√	√
Meeting Template	Meeting templates under an organization or a sub-organization where a user belongs, which can be added.	x	√	√
Ongoing Meetings	Ongoing meetings under an organization or a sub-organization where a user belongs.	x	√	x
Meetings About to Start	Meetings to be held under an organization or a sub-organization where a user belongs.	x	√	x
My Meetings	Meetings scheduled by a user.	x	x	√
Meeting History	Meetings that have been held under an organization or a sub-organization where a user belongs.	x	√	√
Default Settings	Default settings for a meeting.	x	√	√
Personal Information	Information of a user.	x	√	√

## 8.2 Software Upgrade

You can upgrade the SMC on the SMC web interface.

A system administrator can easily upgrade the SMC by uploading an upgrade package.

Before you start:

- Confirm the current system version and the target version.
- Back up the system.
- Ensure that no meeting is ongoing.

During the upgrade: Upload an upgrade package. The upgrade takes about 30 minutes.

Post-upgrade: Log in to the SMC web interface again and check whether the system version is the target one.

## 8.3 Data Backup

You can back up or restore the configuration and service data of the current system with one click on the SMC.

- Data backup: On the SMC web interface, you can back up SMC data with one click. When the backup is complete, a message indicating that the backup is successful is displayed. Additionally, you can download the backup file to a local directory or a third-party server.
- Data restoration: To restore the backup data, reinstall the SMC and then import the backup file.

## 8.4 Logs

You can manage logs on the SMC. These logs are classified into operation logs, security logs, debug logs, meeting logs, and device logs by application scenario.

Logs are one of the most important basic O&M data of a product. During product running, logs can be used for intelligent analysis such as mining and clustering to effectively support maintenance activities such as network fault prediction, subhealth detection, as well as fault demarcation and locating.

[Table 8-2](#) describes SMC logs.



**Table 8-2** SMC logs

Log Type	Log Information	Log-related Operations
Operation Logs	Record the instructions initiated by maintenance personnel or scheduled tasks of the system. These logs are printed during meeting initiation and control, as well as system maintenance performed by system administrators, conference administrators, and common users, and also contain those generated for scheduled tasks. Operation logs include all operation logs except conference operation logs.	These logs can be generated, stored, queried, or exported.  Operation logs are centrally stored in databases. System administrators or maintenance personnel can query operation logs by condition on the system configuration page. In addition, operation logs can be exported for maintenance personnel to locate faults.
Security Logs	Record system users' (including system administrators, maintenance personnel, and system monitoring personnel) activities such as login, logout, authorization, adding/deleting users, locking/unlocking users, changing role permissions, modifying system security configurations.	These logs can be generated, stored, queried, or exported.  Security logs are centrally stored in databases. System administrators can query operation logs by condition on the system configuration page. In addition, security logs can be exported for maintenance personnel to locate faults.
Debug Logs	Record code-level information. Generally, debug logs are used to trace running paths, for example, recording the entry and exit of functions, for product R&D personnel to locate complex problems. Most debug logs are code-level information.	Debug logs can be generated, stored, and exported.  Debug logs are stored in disk files. System administrators or authorized users can export debug logs for fault locating and analysis.

Log Type	Log Information	Log-related Operations
Meeting Logs	Record conference operations (including conference initiation and control) performed by conference administrators or common users. Similar to operation logs, the SMC records conference logs separately to facilitate conference control management performed by conference administrators or common users.	These logs can be generated, stored, queried, or exported. Conference logs are centrally stored in databases. Conference administrators or common users can query the logs on the <b>Meeting History</b> or <b>Meetings About to Start</b> pages. In addition, conference logs can be exported for maintenance personnel to locate faults.

**Table 8-3** Log levels

Log Level	Device Name	Description
fatal	Fatal error	Indicates that system services are severely damaged or completely unavailable and a large number of users are affected. In this case, O&M personnel need to handle the issue immediately.
error	Critical error	Indicates that the system running environment or functions are affected, or function execution errors occur due to unexpected data or events. For example, data fails to be imported to the database or a task fails to be created.
warn	Warning	Indicates that the system has potential risks, but the risks do not affect system functions. For example, if an error occurs during data verification, the system rectify this error using the error correction function, which does not affect the function execution.
info	Information	Records the information about the system normal running, including status or state changes. For example, the current system status and database connection status will be recorded.
debug	Debug	Traces running paths and records debugging information, for example, tracing entry and exit of functions. The logs help developers to locate complex problems. In addition, the logs of this level also record code information, such as functions and parameters that are currently invoked, internal variable values, and the return values of invoked functions. Related information existing before an exception occurs or an error message is returned are recorded.

## 8.5 Alarms

You can configure, report, clear, query, and dump alarms on the SMC with a comprehensive alarm system.

An alarm is a notification generated when the system detects unexpected status and requires user intervention. The alarm system consists of five key modules: front-end control platform, alarm configuration library, alarm storage platform, core alarm processing layer, as well as fault and time capture and alarm triggering layer.

- Front-end control platform: allows users to query and modify alarm configurations, query or clear current alarms, and query or delete historical alarms.
- Alarm configuration library: stores alarm configurations.
- Alarm storage platform: stores current and historical alarms.
- Core alarm processing layer: processes alarm events, queries and clears alarms, determines repeated alarms, sends alarm emails and SMS messages, as well as processes alarm configurations.
- Fault and time capture and alarm triggering layer: captures faults and events in service events and generates alarm events. The alarm management module listens to alarm events and generates alarms accordingly.

### Alarm Classification

- Current alarms: refer to uncleared alarms.
- Historical alarms: refer alarms that have been cleared.

### Alarm Status

- **Cleared:** indicates that the fault for which the alarm is generated has been rectified. **Cleared** represents the state of an alarm, while **Repair** and **Correct** indicate a fault state. **Restore** indicates that the device status and capability are restored to a normal state. After a fault is rectified, the alarm is cleared in the management system.
- **Active:** indicates that the alarm has not been cleared. Active alarms indicate that exceptions still exist and should be focused on during routine maintenance.

## 8.6 One-click Information Collection

You can export locating information with one click on the SMC.

Information collection is available to the following devices:

- SMC
- CloudMCU/VP9800 series MCU
- VP9600 series MCU
- CloudRSE

- TE series/TX50 endpoints
- DP300 endpoints
- Bar/Board/Box series endpoints
- RoomPresence series endpoints
- RP100/RP200
- IdeaHub

On the SMC web interface, you can collect NE information with one click. After the collection is complete, download the collected information for R&D personnel to locate faults.

## 8.7 Device Upgrade

You can upgrade manageable Huawei devices on the SMC.

The upgrade is available to the following devices:

- TE series/TX50 endpoints
- DP300 endpoints
- Bar/Board/Box series endpoints
- RoomPresence series endpoints
- RP100/RP200
- IdeaHub series

To upgrade a device, upload the device version file to the SMC. The SMC then controls the device to be upgraded. With the SMC, you can also upgrade devices in batches.

## 8.8 Device Inspection

You can inspect manageable devices on the SMC.

The inspection is available to the following devices:

- SMC: self-check
- SC
- MCU: VP9000 series MCU and CloudMCU
- CloudRSE
- Endpoints: TE series endpoints (including TE10, TE20, TE30, TE40, TE50, and TE60), TX50, RP100/200, Bar 300/500, Board, Box 300/500/600/700/900, RoomPresence series endpoints, Board2, and IdeaHub Pro/S.

Before inspecting a device, download an inspection template, modify the inspection items in the template, and then upload the template to the SMC. You can select overall or partial inspection.

# 9 Technical Specifications

This section describes the physical specifications and performance indicators of the SMC, as well as the standards that the SMC complies with.

## 9.1 Performance Specifications

This section describes the performance specifications of the SMC and SC.

[Table 9-1](#) describes the performance specifications of the SMC. [Table 9-2](#) describes the performance specifications of the SC.

**Table 9-1** Performance specifications of the SMC

Type	Specification	Co-deployment	Standalone Deployment
User and meeting room	Maximum number of meeting rooms and users	10,000	200,000
	Maximum number of concurrent online users	500	5000
Device	Number of MCUs	50	512
	Number of SCs	5	64
	Number of recoding and streaming servers	50	128
Terminal	Number of manageable endpoints	10,000	50,000
Organization	Highest organization level supported	Level 8	Level 8

Type	Specification	Co-deployment	Standalone Deployment
	Maximum number of supported organization nodes	200	500
Region	Highest region level	Level 8	Level 8
	Maximum number of area nodes (departments)	200	500
Meeting	Maximum number of sites in a single conference	300	3000
	Number of conference templates	Total number of meeting templates: 1000 Max. number of templates for a meeting administrator: 200 Max. number of meeting templates for a common user: 10	Total number of meeting templates: 200,000 Max. number of templates for a meeting administrator: 200 Max. number of meeting templates for a common user: 10
	Maximum number of concurrent scheduled meetings	2,000	40,000
	Maximum number of concurrent scheduled sites	10,000	200,000
	Maximum number of concurrent active meetings	1000	5000
	Maximum number of concurrent active sites	1000	20,000
	Cascaded conference	Maximum number of concurrent cascaded meetings	20
Highest meeting level		Level 4	Level 4
Number of multi-level conference templates		200	500

**Table 9-2** Performance specifications of the SC

Specification	Co-deployed SC (CloudLink Edge 1000)	Co-deployed SC (Medium-capacity)	Standalone SC
Number of registered devices	1000	10,000	10,000
Call capacity	500 signaling routes 1000 calls in total	1000 signaling routes 1000 calls in total	3000 signaling routes 6000 calls in total
Traversal traffic	60 Mbit/s	60 Mbit/s	Single network port: 400 Mbit/s Dual network ports: 600 Mbit/s

## 9.2 Standards and Protocols Compliance

This topic describes the standards and protocols compliance of SMC.

**Table 9-3** lists the standards and protocols that the SMC complies with.

**Table 9-3** Standards and protocols compliance

Item	Standard and Protocol	Involved Specifications
Multimedia frame protocol	ITU-T H.323	-
	IETF SIP	RFC3261 and extensions
Other standards and protocols	TCP/IP	RFC793
	HTTP	RFC1945, RFC2616, RFC2818
	HTTPS	RFC2818
	SSH	RFC4250-4256, RFC4335, RFC4344, RFC4345
	SNMP	<ul style="list-style-type: none"> <li>• RFC1065-1067, RFC1155-1157, RFC1214</li> <li>• RFC1441-1452, RFC1901-1910</li> <li>• RFC3411-3418</li> </ul>

Item	Standard and Protocol	Involved Specifications
	SOAP	W3C (World Wide Web Consortium) SOAP1.2
	LDAP	RFC4511-RFC4519, RFC4370, RFC2696, RFC2891, RFC2830
	DNS/DDNS	RFC1034, RFC1035
	H.350	-
	RTP	RFC3551, RFC3853, RFC3711, RFC4568
	RTCP	RFC3550
	H.225	-
	H.245	-
	Q.931	-
	H.235	-
	SDP	-
	TLS/SRTP	-
	H.239	-
	BFCP	RFC4582
	H.460	-
	ICE	-
	STUN	-
	TURN	-
	SNP	-
	SIP TRUNK	-



# 10 Acronyms

---

Acronym	Full Name
CPU	Central Processing Unit
DMZ	Demilitarized Zone
SC	Switch Center
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IVR	Interactive Voice Response
LDAP	Lightweight Directory Access Protocol
MCU	Multipoint Control Unit
SIP	Session Initiation Protocol
SMC	Service Management Center
SOAP	Simple Object Access Protocol
XML	Extensible Markup Language