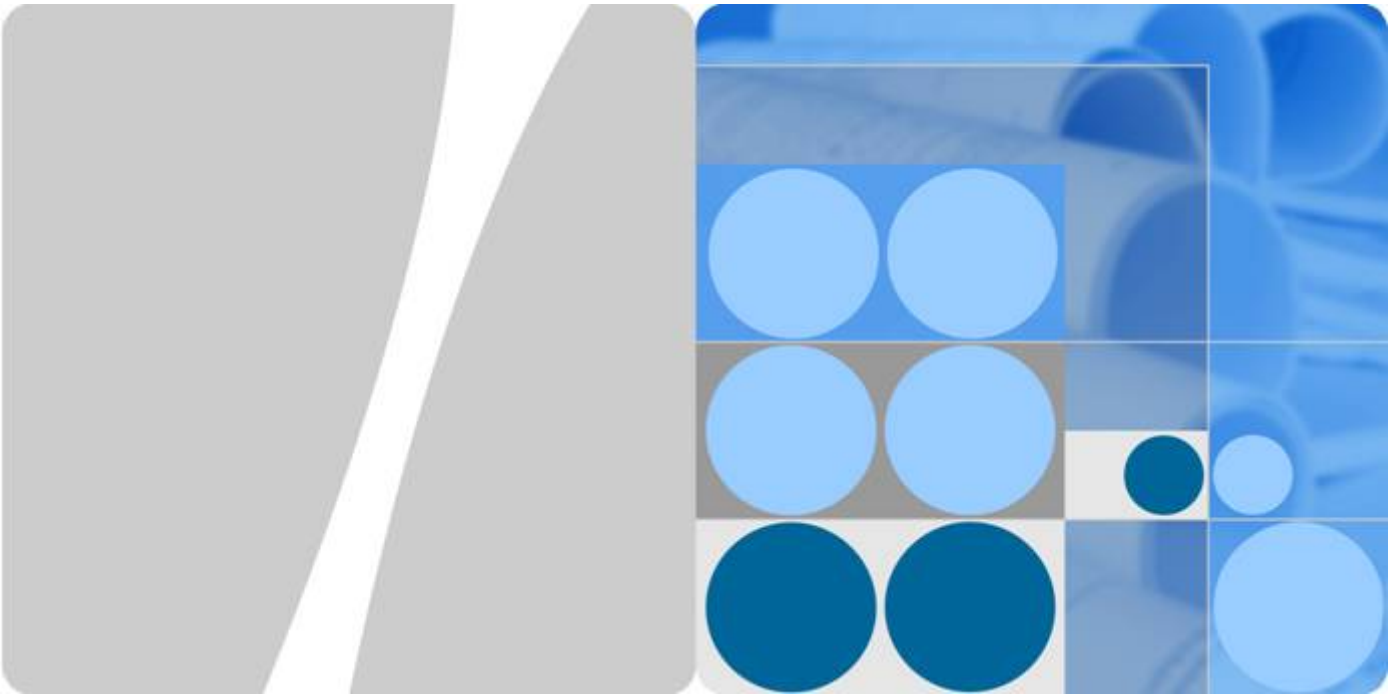


CloudECS

V600R006C10

Product Overview

Issue 01

Date 2018-07-09

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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

Contents

1 Product Positioning

With the rapid development of Internet communication, the requirements on communication convenience and efficiency increase, and voice calls cannot meet communication requirements of enterprise users. Enterprise users require more communication modes. As an enhanced communications suite for the Cloud Enterprise Communications (CloudEC) and Cloud Private Branch Exchange (CloudPBX) solutions, the Cloud Enhanced Communications Suite (CloudECS) complies with the development trend and provides rich unified communications (UC) services for enterprise users, such as the message, group, and presence services.

2 Product Features

Extensive Services

- Supports UC soft client access.
- Provides the message, group, and presence services.
- Supports offline messages. When a user is offline, the server buffers messages sent to the user and sends the messages to the user once the user goes online.
- Supports rich media messages to enrich users' message communication experience. A rich media message is a multimedia message extended based on the instant text message. Rich media messages include pictures, voice clips, and video clips.
- Supports mobile communication. A user who is not in the office can use the Mobile Client to smoothly communicate with other colleagues using the message, call, and conference services, implementing mobile office.

Flexible Deployment for Adapting to Multiple Network Scenarios

- The following deployment modes are supported, allowing flexible deployment and elastic capacity expansion, improving device usage, and reducing O&M costs.
  - E9000 server + FusionSphere NFV cloud platform
  - RH2288 server + CGP virtualization platform
  - Common server + VMWare
- Supports hosted and on-premises networks. Enterprises can deploy the CloudECS based on the user capacity and service scope, reducing the initial investment. Later, they can smoothly expand the capacity as required, protecting the existing investment.

Convenient Management and Maintenance

Provides the business management unit (BMU) for system management and maintenance.

- Supports system configuration, interworking configuration, and log tracing.
- Supports plug-in parameter management and uses plug-in parameters to control UC soft clients in the network-wide manner.
- Supports version upgrade policy delivery for automatically upgrading UC soft clients.
- Supports log tracing for UC soft clients, improving troubleshooting efficiency.

High Reliability

The system supports two-node cluster, cluster, and DR deployment mode, ensuring reliable system running.

3 System Architecture

The CloudECS consists of the following functional modules: eServer, mobile access agent (MAA), unified media server (UMServer), BMU, and DB. Each module independently provides service capabilities and also cooperates with other modules to ensure proper running of UC services.

Figure 3-1 CloudECS functional modules

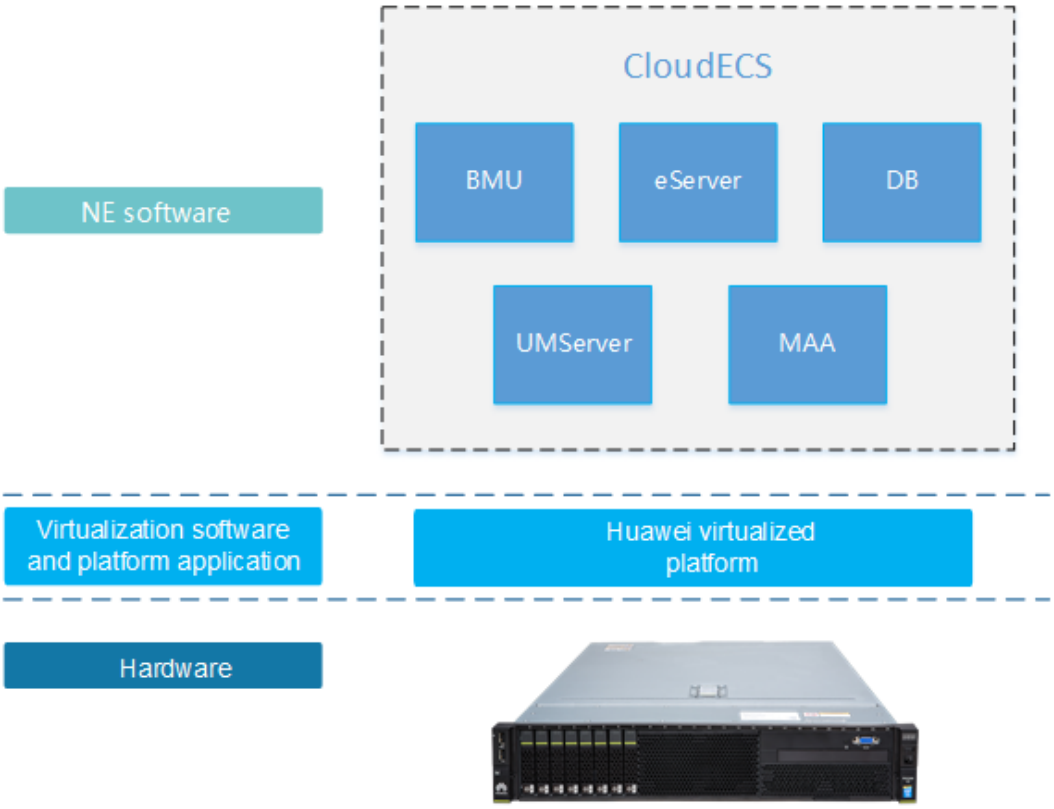


Table 3-1 Description of CloudECS functional modules

Functional Module	Description
eServer	Provides account registration, authentication, instant messaging (IM), presence, and group functions for the Desktop Client and Mobile Client.
MAA	Provides access for the Mobile Client. When the Mobile Client initiates a registration request, the MAA checks whether the UC account has the rights to use the Mobile Client. If the UC account can use the Mobile Client, the MAA forwards the registration request to the eServer.
UMServer	Provides rich media message functions that allow users to send pictures, voice clips, and video clips to each other. Additionally, the UMServer provides the offline file transfer function for the Desktop Client. The typical configuration and retention policy for the UMServer space are as follows, which can be adjusted based on the service requirements: ● Common rich media data: 50 MB for each user. Rich media data of each user is stored for a maximum of seven days. ● Group file sharing: 200 MB is required for each user. Group files are managed by users on the eSpace Desktop, and the system does not automatically delete such files. ● Work Community: 50 MB is required for each user. Work Community files are not deleted by default. (To prevent the hard disk space from being used up, a customer needs to configure periodical deletion of Work Community files on the BMU.)
BMU	Provides a management portal that supports a variety of CloudECS management functions, including Desktop Client and Mobile Client upgrade policy management, CloudECS service parameter management, and management of interworking between CloudECS servers and peripheral NEs.
DB	Stores data such as directories, groups, messages, logs, and NE configurations. In a scenario where there are more than 2000 users, the Oracle database needs to be used. In a scenario where there are less than 2000 users, the MySQL database can be used.

4 Hardware and Software Requirements

The CloudECS supports virtualization deployment based on Huawei RH2288. The hardware and software planning varies according to the user capacity.

Capacity	Server	Quantity	Hardware		Operating System	Remarks
0 to 2000 users	EC_ECS_ALL_S	1-2	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	CloudECS service modules are jointly deployed on the same VM. The MySQL database is used and is independently deployed on a single VM.

Capacity	Server	Quantity	Hardware		Operating System	Remarks
2,000 to 10,000 users in single-node system or two-node cluster deployment	EC_ECS_AIO_Server	1-2	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	The Oracle Single database is deployed in a single-node system. Local disks are used. The Oracle RAC database is deployed in a two-node system. It needs to connect to external SAN storage (the OceanStor 2600 V3 is recommended).
10,001 to 40,000 users in two-node cluster deployment	EC_ECS_BASE_A_Server	2	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	The Oracle RAC is used by default. It needs to connect to external SAN storage (the OceanStor 5500 V3 and the OceanStor 5500 V5 are recommended).

Capacity	Server	Quantity	Hardware		Operating System	Remarks
	EC_ECS_BASE_B_Server	2	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	-
40,001 to 400,000 users in two-node cluster deployment	EC_ECS_BMU_Server	2	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	-

Capacity	Server	Quantity	Hardware		Operating System	Remarks
	EC_ECS_BASE_B_Server	2-11	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	-
	EC_ECS_EXTEND_Server	n	RH2288 V3 2 x E5-2618L v4 CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter SR130	2288H V5 2*Xeon Silver 4114-10Core CPU 8 x 16 GB memory 6 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350) SR450C	SUSE Linux 11 SP3	-

Capacity	Server	Quantity	Hardware		Operating System	Remarks
	EC_ECS_DB_Server	2	RH2288H 2 x E5-2697A v4 CPU 32 x 16 GB memory 4 x 600 GB SAS disk DVD-RW 4 x GE, 1 x 4-port network adapter	2288H V5 2 x Xeon Gold 6130T-16Core CPU 16 x 32 GB memory 4 x 600 GB SAS disk DVD-RW 2 x GE + 2 x 10GE optical ports (excluding optical module), 4 x GE electrical ports (I350)	SUSE Linux 11 SP3	The Oracle RAC needs to be independently deployed on a high-spec server. It needs to connect to external SAN storage.

If the number of mobile clients, concurrent rich media channels, or concurrent multimedia conference participants does not meet requirements, you can add the EC_ECS_EXTEND_Server to flexibly deploy the MAA, UMServer, or MS VMs in single-node systems or clusters.

In the on-premises scenario, the number of VMs that can be deployed on a single EC_ECS_EXTEND_Server must comply with the following formula: (A x 1) + (B x 0.6) + (C x 1) ≤ 2.6, where 0 ≤ A (number of UMServer VMs), B (number of MAA VMs), and C (number of MS VMs) ≤ 4. In the hosted scenario, the number of VMs that can be deployed on a single EC_ECS_EXTEND_Server must comply with the following formula: (A x 1) + (B x 0.6) ≤ 2.6, where 0 ≤ A (number of UMServer VMs) and B (number of MAA VMs) ≤ 4. Therefore, VMs can be added flexibly. The following uses adding of UMServers as an example.

Rich Media Channel Adding Plan	0 ≤ Number of Users/Devices < 2000	2000 ≤ Number of Users/Devices < 10,000	10,000 ≤ Number of Users/Devices < 40,000	40,000 ≤ Number of Users/Devices < 400,000
Database requirements	No SAN storage needs to be deployed if the database is deployed in a two-node cluster. No independent NAS storage needs to be deployed for rich media functions. By default, only 200 GB storage space is available. If larger storage space is required, customers need to prepare NAS storage (2600V3 is recommended) themselves.	Independent SAN storage (2600V3 is recommended) must be deployed if the database is deployed in a two-node cluster. If rich media functions are required, independent NAS storage (2600V3 is recommended) must be deployed. In the on-premises scenario where there are 10,000 users, the database shares the same 2600V3 storage with the SAN.	Independent SAN storage (5500V3 is recommended) must be deployed if the database is deployed in a two-node cluster. Independent NAS storage (5500V3 is recommended) must be deployed if rich media functions are required.	Independent SAN storage (5500V3 is recommended) must be deployed if the database is deployed in a two-node cluster. The IP SAN is recommended as SAN storage. For better SAN reliability, the FC SAN can be deployed. Independent NAS storage (5500V3 is recommended) must be deployed if rich media functions are required.
Number of concurrent rich media channels	40	40	150	150
Number of servers	1 or 2	1 or 2	1 or 2	1-10 or 2-11
Number of UMServer VMs on each server with typical configurations	1	1	1	1
Number of VMs to be added	No VM can be added in a small-capacity scenario.	0-2	0-2	0-2

NOTE

Remote DR is supported. If the system is deployed in DR mode, after the number of servers required at a single site is calculated, the total number of servers required needs to be doubled.

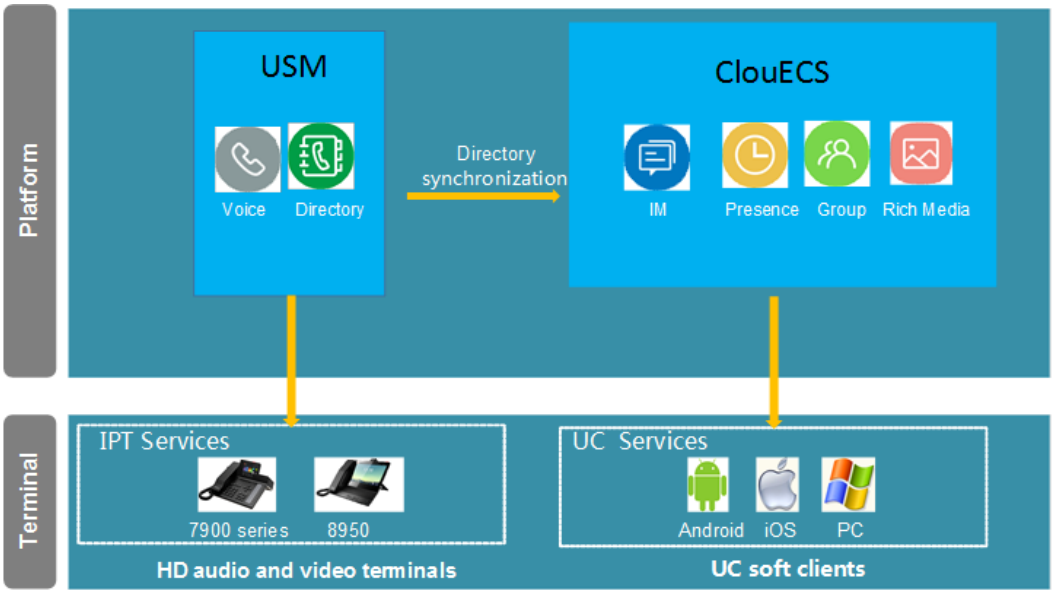
5 Application Scenarios

The CloudECS supports multiple network modes to provide UC services for users in different application scenarios.

5.1 Enterprise On-Premises Scenario

The enterprise on-premises network is oriented to fields such as the government, transportation, security, finance, large-sized enterprise, and small- and medium-sized enterprise (SME). The enterprise on-premises network provides IP telephony (IPT), UC, and conference services, among which IPT services and UC services are loosely coupled. An enterprise can use IPT services without deploying the CloudECS. The CloudECS needs to be deployed only when the enterprise needs to use UC services.

Figure 5-1 On-premises scenario

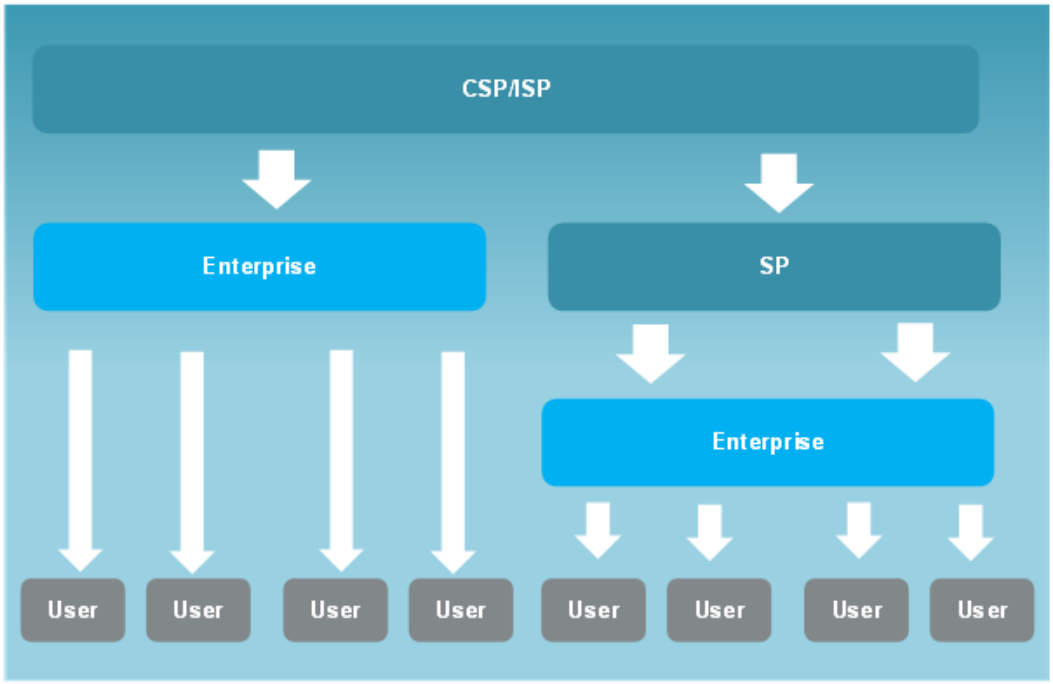


5.2 Hosted Leasing Scenario

The CloudECS can be used on the hosted network and supports the multi-tenant scenario where UC services are leased to enterprises.

Function	Description
Tenant data isolation	One CloudECS system can provide UC services for multiple tenants at the same time. All tenants' information is stored in the same Oracle database. The enterprise ID is used to identify and distinguish different tenants' data. Tenants are isolated based on service logic when they access CloudECS services.
Tenant isolation in service access	Tenants are strictly isolated when they access CloudECS services, including corporate directory access, point-to-point (P2P) and group message sending, P2P file transfer, group query, group shared file query, and Work Community invitation.
Multi-tenant log audit	Logs, including IM, login, P2P file transfer, short message service (SMS), and rich media file upload and download logs, can be audited by tenant.
Multi-tenant system bulletins	System bulletins can be sent by tenant.

Figure 5-2 Hosted operation mode



6 Functions and Features

The CloudECS provides rich UC functions to help enterprise users collaborate and communicate more conveniently.

Figure 6-1 CloudECS services

6.1 IM

The CloudECS provides the IM function for enterprise users to communicate with each other anytime and anywhere.

Function	Description
Online message	● Clients can send and receive IMs online, including P2P and group messages. ● IMs are in HTML format, and can contain text, emoticons, small pictures, and rich media URLs. ● In the mobile rich media scenario, voice and video clips, doodles, pictures, and photos taken instantly can be sent in IMs.

Function	Description
Offline message	● If the recipients are offline, the message server stores messages temporarily and sends the messages to the recipients when they get online. ● If offline messages contain rich media URLs, clients download rich media files from the UMServer. ● Offline messages are stored for a maximum of seven days and then will be deleted.
Unread message	● If a P2P message, a group message, a system bulletin, or an SMS message is not read by an online user, the user can still receive the message upon the next login. ● If unread messages contain rich media URLs, clients download rich media files from the UMServer.
Historical message roaming	● P2P messages, group messages, system bulletins, and SMS messages sent or received by users are stored on the message server. Users can obtain historical messages on different clients. ● If historical messages contain rich media URLs, clients download rich media files from the UMServer. ● Historical messages are stored for a maximum of 30 days and then will be deleted. This duration cannot be adjusted. As restricted by the UMServer storage space under typical configurations, common rich media files are stored for seven days by default. That is, rich media files of messages sent seven days before cannot be obtained.
SMS message	The system supports text SMS message exchange between the Desktop Client and mobile phones (in the circuit switched domain). In the P2P or group message window on the Desktop Client, a user can switch to the SMS mode to send SMS messages. Replies to the sent SMS messages will be received by the Desktop Client. A signature can be set for SMS messages. After a successful setting, each SMS message automatically carries the signature. The default signature is the user name. The CloudECS does not provide any SMS gateways. An enterprise needs to provide an SMS access gateway to connect to the uPortal. When the Desktop Client sends SMS messages, the CloudECS sends SMS message forwarding requests to the uPortal. The SMS gateway supports the SMPP3.4 standard protocol, CMPP3.0 protocol used by China Mobile, and SMGP2.0 protocol used by China Telecom.
Message pushing	If new messages are received when the Mobile Client for iOS is running at the background or the process of the Mobile Client for Android is terminated, the message server automatically pushes message notifications to users' mobile phones to notify users of the new messages.

Function	Description
Screenshot on the Desktop Client	Users can take a screenshot of a specified area on the screen or copy a picture from the Windows clipboard and send the screenshot or picture to peer parties. This function can be used in P2P or group chats.

Figure 6-2 P2P IM chat

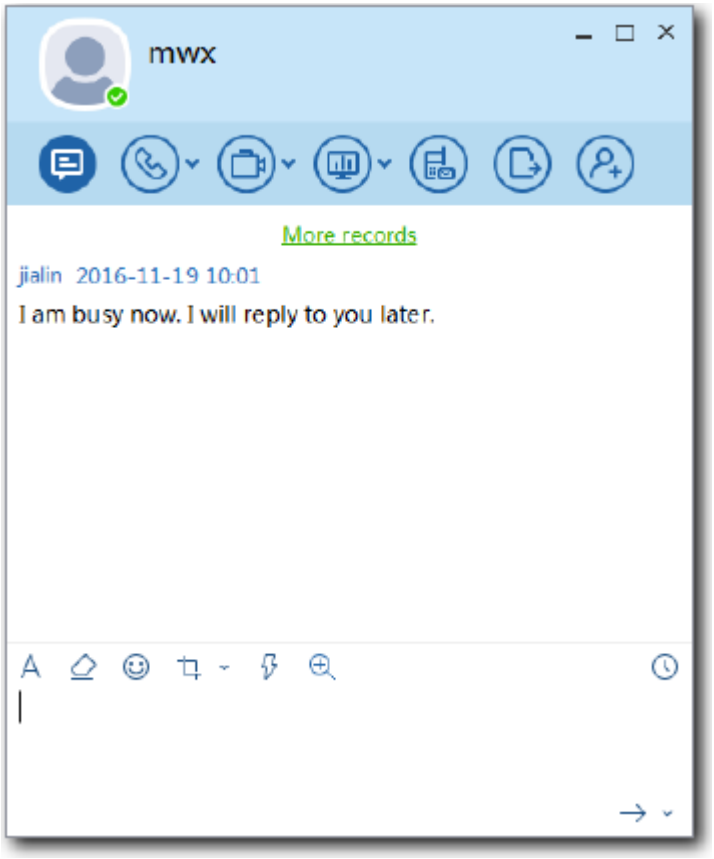


Figure 6-3 File transfer

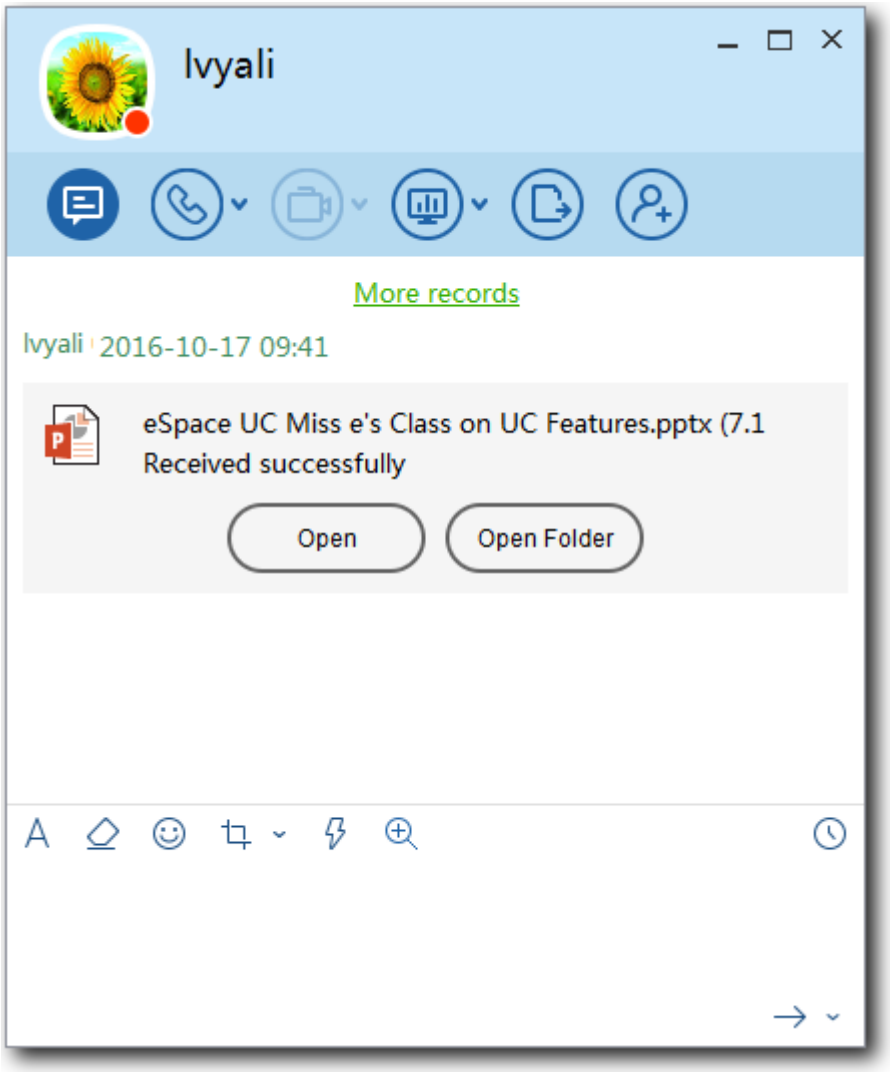
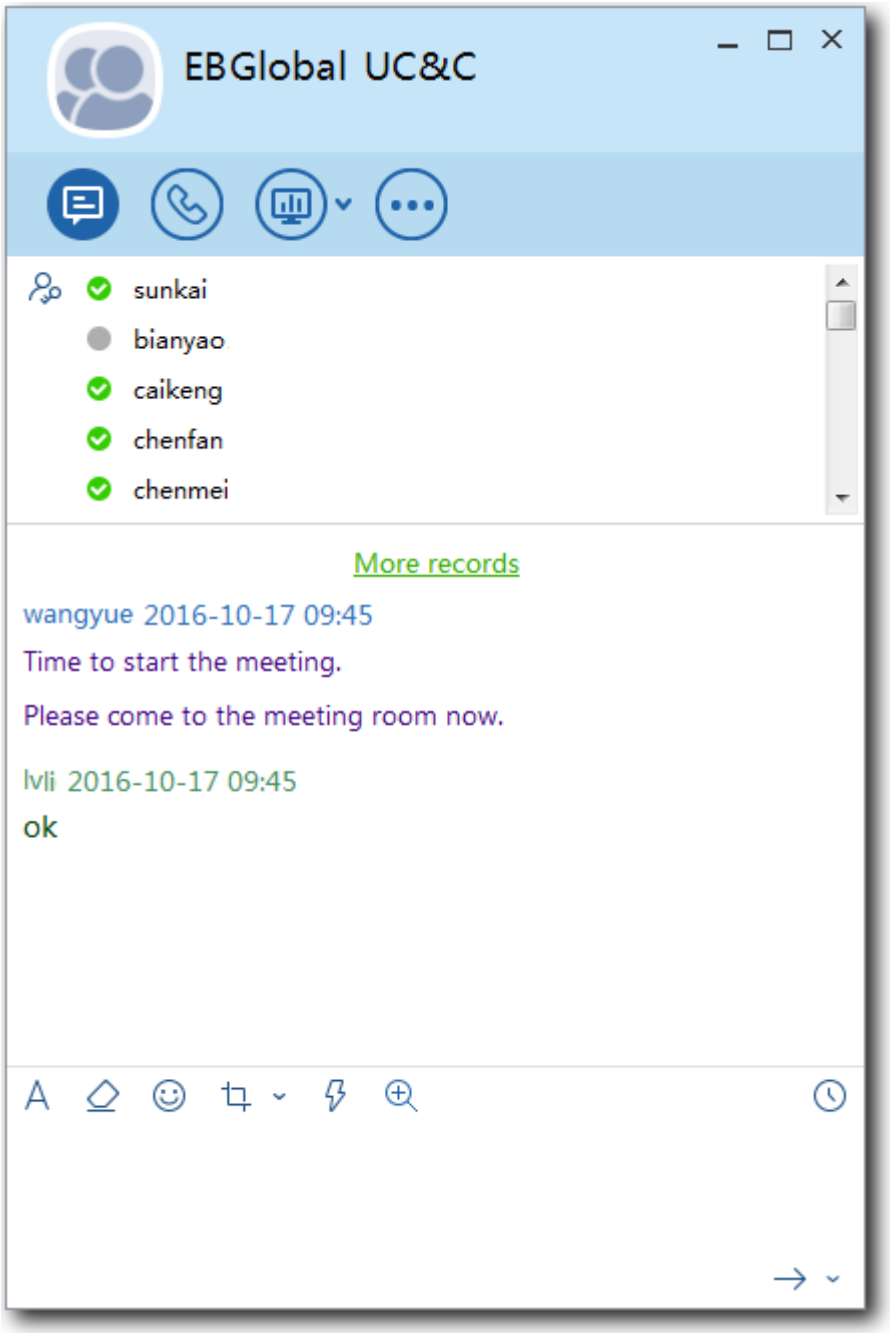


Figure 6-4 Group chat

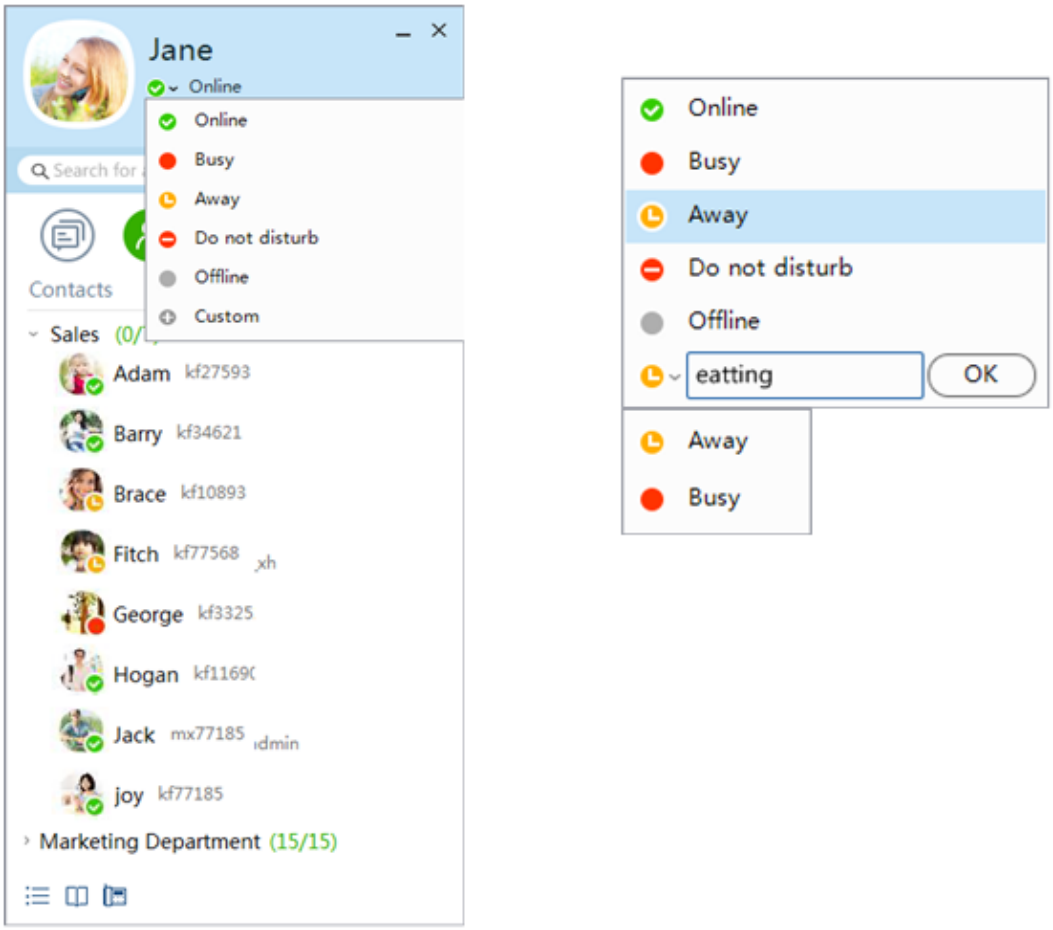


6.2 Presence

The CloudECS provides the presence function for UC soft clients so that users can select the appropriate communication method based on the contact status.

Function	Description
Status releasing and notification	● After a user releases the status on a client, the system pushes the status change to the user's online contacts in real time to notify these contacts of the user's current status. ● User states include offline, online, busy (calling or in-conference), away, and do not disturb (DND). ● Users can customize secondary away and busy states on the Desktop Client.
Signature	After a user sets a signature on a client, the system pushes the signature to the user's online contacts in real time.
Profile picture	After a user sets a profile picture on a client, the system pushes the profile picture to the user's online contacts in real time.
Contact information change notification	After a user modifies personal information on the personal portal, the system pushes the information change to the user's online contacts after a period of time. The system pushes incremental information changes at an interval of 10 minutes.

Figure 6-5 Presence



6.3 Group

Users can add specific contacts to a group to facilitate multi-party communication and group file sharing and improve multi-party office collaboration capabilities.

Function	Description
Creating a group	● Users can create groups on clients, including contact groups and temporary groups. ● Contact groups apply to the scenarios where relatively fixed management rights are required. Only the group administrator can manage the group, including inviting and deleting members, modifying group information, and modifying member rights. ● Temporary groups apply to the scenarios where open management rights are required. All members can invite other contacts and modify the group name; however, only the group administrator can delete members. When a user creates a multi-party chat on the Desktop Client, the system automatically generates a temporary group.
Dismissing a group	● The administrator of a contact group can dismiss the group. ● If a temporary group is inactive for 60 days, the system automatically dismisses it.
Modifying group information	● The group information of a contact group, including the group name, introduction, bulletin, and authentication setting, can be modified only by the group administrator. ● All members of a temporary group can modify the group name. ● After the group information is modified, the system notifies all online group members in real time.
Searching for a group	This function is supported only by the Desktop Client. ● Users can search for a contact group by group name or group ID on clients. ● The search by group name is conducted in fuzzy mode, while the search by group ID is conducted in exact mode.
Inviting a user to a group	● The administrator of a contact group can invite users to the group. Each invited user will receive a notification and can directly join the group. ● All members of a temporary group can invite users to the group. ● After group members change, the system notifies all online group members in real time.
Deleting a group member	● The administrator of a contact group can delete a group member. ● The administrator of a temporary group can delete a group member. ● After group members change, the system notifies all online group members in real time.

Function	Description
Quitting a group	● Group members can quit their group. The quit operation does not need approval of the group administrator. If the group administrator quits the group, the system randomly selects a group member as the new group administrator. ● After group members change, the system notifies all online group members in real time.
Transferring the administrator rights	This function is supported only by the Desktop Client. ● The group administrator can transfer the administrator rights to a group member. ● After the group administrator changes, the system notifies all online group members in real time.
Adding a group to favorites	● Users can add temporary groups to favorites on clients. Temporary groups added to favorites are displayed in the group list. ● Temporary groups not added to favorites are displayed only in recent chats and historical records.
Locking a temporary group	The group administrator can lock a temporary group to convert it into a contact group and unlock the contact group to restore it as a temporary group.
Sharing files in a group	This function is supported only by the Desktop Client. ● Each group is allocated with a shared file space of certain capacity. Group members can upload files to and download files from the group space, and view and search for group shared files. ● The group administrator can set the maximum size of a single file that can be uploaded. (The maximum size cannot exceed that configured in system settings.) When group members upload files to the group space, the file size cannot exceed this limit. ● The group administrator can delete all files uploaded to the group space, while group members can delete only files uploaded by themselves. ● The group file list supports search by file name or file type. If clients are offline or users have not logged in to clients, the system searches for only files that have been downloaded locally; if clients are online, the system searches for files on the CloudECS server. The group file list supports filtered display by format, including documents, pictures, media (video and music), and others.
@ function	This function is supported only by the Mobile Client. A user can @ a group member in the group chat, and the group member is notified of the @ message. The @ message is visible to all group members in the group chat.

Figure 6-6 Group operations

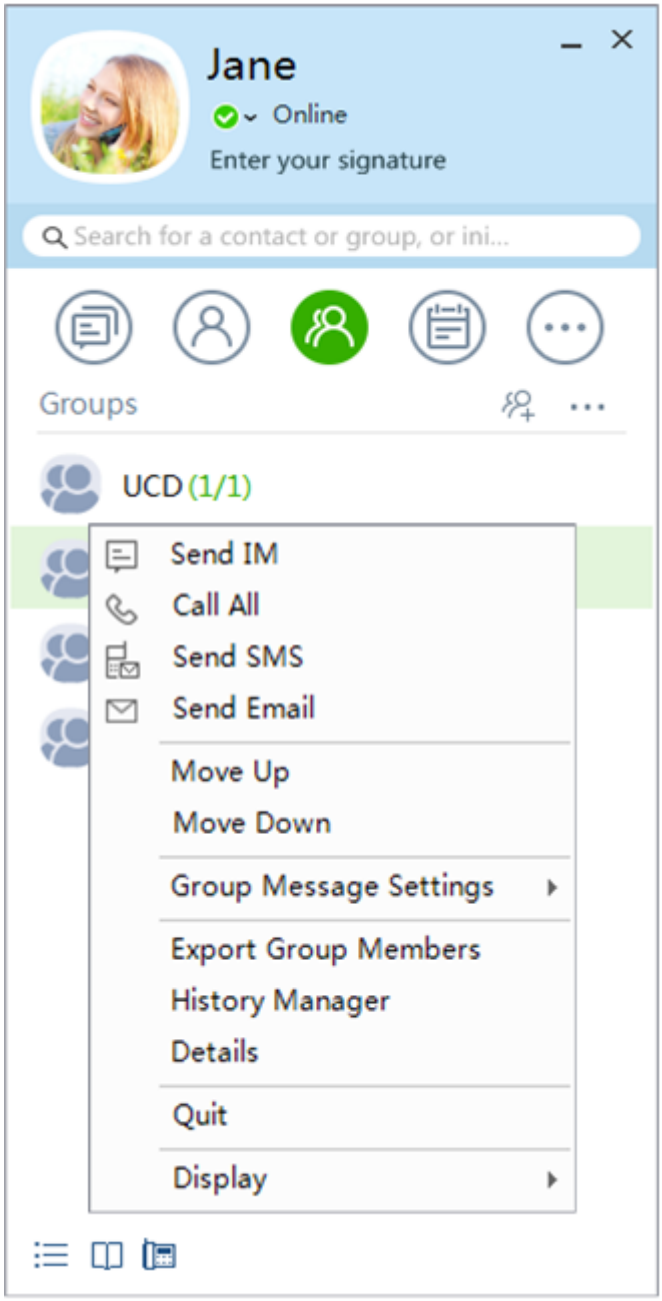
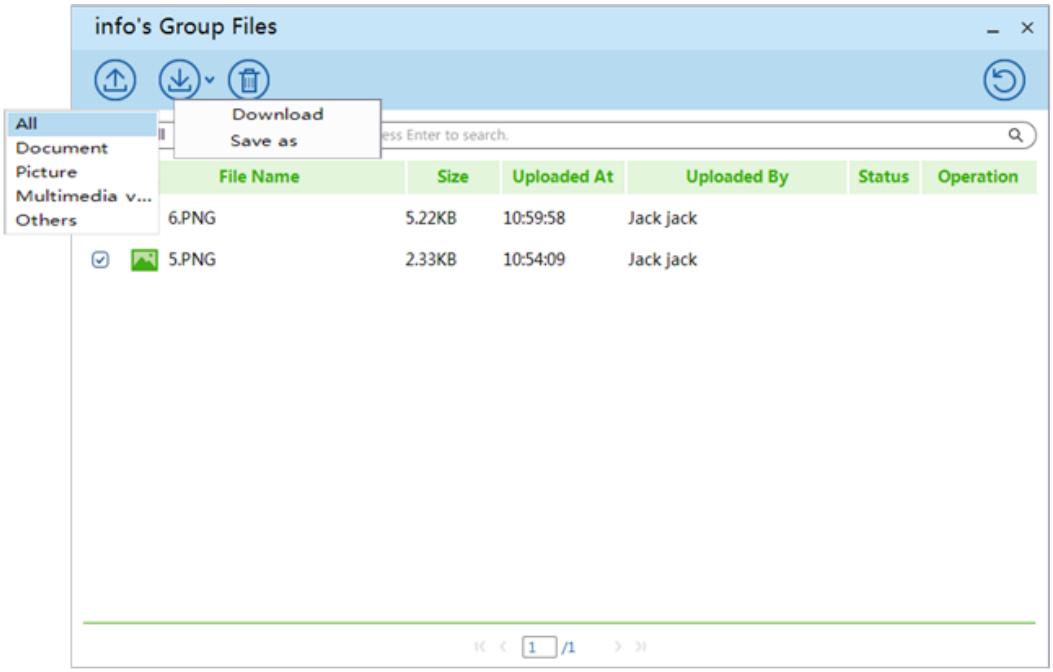


Figure 6-7 Group files



6.4 File Transfer

The CloudECS provides the file transfer function, which allows online users to use the Desktop Client to send files or folders to other users in online or offline mode.

Function	Description
Online file transfer	● Two online clients can transfer files to each other. ● If the two online Desktop Clients can directly communicate with each other, P2P file transfer is used preferentially. In file transfer, the signaling is forwarded by the server while data is transmitted directly between the two clients. ● If the two Desktop Clients cannot directly communicate with each other or file transfer is between a Desktop Client and a Mobile Client, the UMServer mode is used. That is, the sender uploads the file to the UMServer and the system sends a notification to the recipient, telling the recipient to download the file from the UMServer. ● The types of files that are prohibited are configurable. No default settings are provided. ● As restricted by the UMServer storage space under typical configurations, the system automatically deletes rich media files that have been stored for over seven days by default. The duration for storing rich media files is a system-level parameter that can be set. To prolong this duration, customers must first ensure sufficient UMServer space.

Function	Description
Offline file transfer	● Files can be sent to an offline user. ● In offline file transfer, the file is first uploaded to the UMServer; when the recipient goes online, the recipient receives an offline file transfer notification and can choose to download the file. ● The types of files that are prohibited are configurable. No default settings are provided. ● As restricted by the UMServer storage space under typical configurations, the system automatically deletes rich media files that have been stored for over seven days by default. The duration for storing rich media files is a system-level parameter that can be set. To prolong this duration, customers must first ensure sufficient UMServer space.
Folder transfer	If the two Desktop Clients can directly communicate with each other, folder transfer between the two clients is supported.

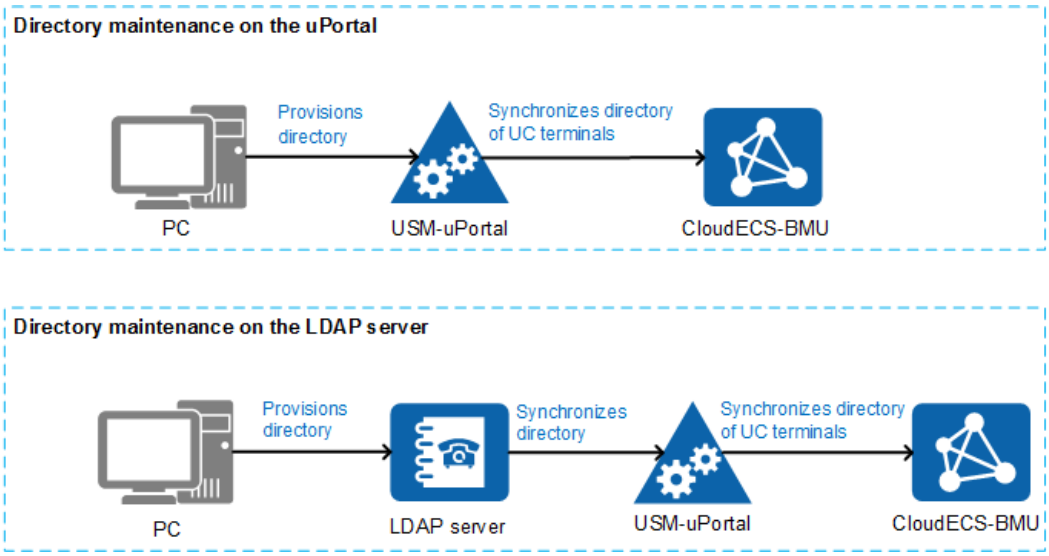
6.5 Directory

Corporate Directory

The corporate directory is a network directory that stores department and contact information. Enterprise users can quickly query enterprise contacts on UC soft clients through the corporate directory in different office scenarios. The system uses LDAP to synchronize corporate directory data from the AD or OpenLDAP server.

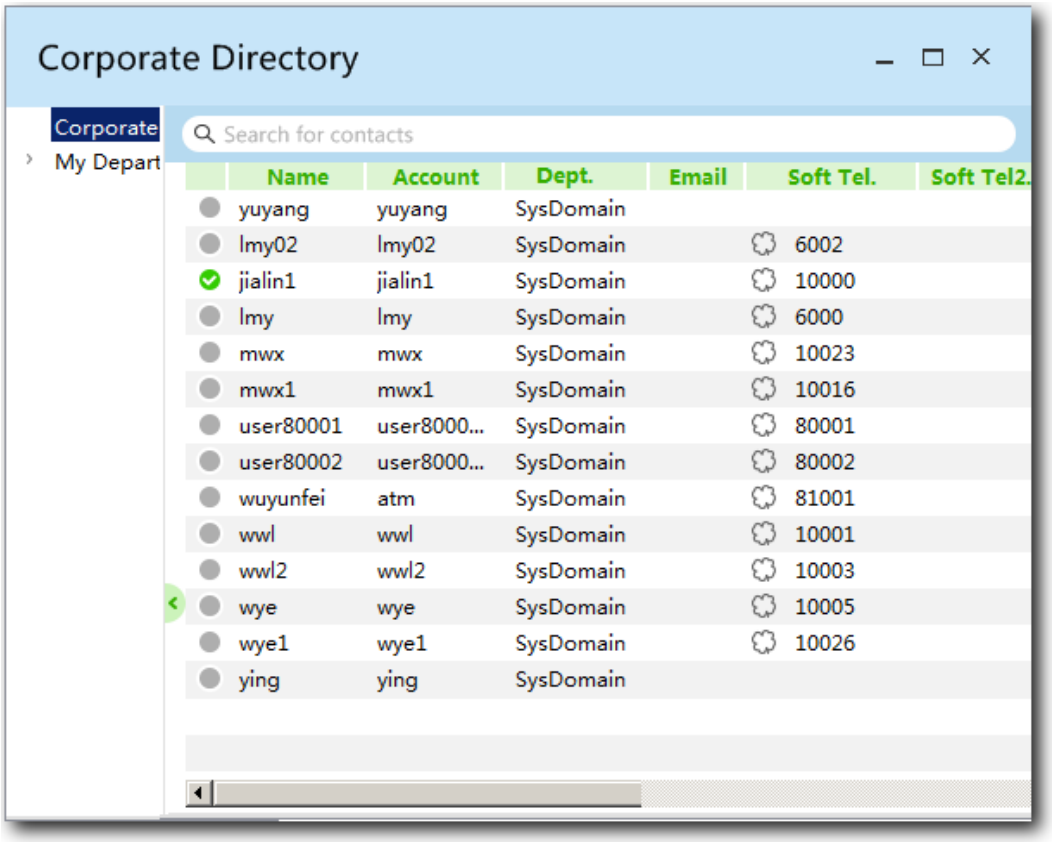
The system administrator maintains directory information on the USM-uPortal. The UC directory is synchronized from the uPortal to the BMU. UC soft clients query contact information in the corporate directory through the eServer.

Figure 6-8 Synchronizing directory data



Function	Description
Single-keyword search	The system supports single-keyword search. Users can search for all enterprise employees or specify a department (including the sub-department) for the search. ● The following fields use the exact match mode: soft client number, mobile number, fixed-line number, short number, home number, other number, other number 2, email, and initials. ● The following fields use the fuzzy match mode: address and department description. ● The following fields use the left match mode: name, account, and pinyin.
Multi-keyword search	The system supports multi-keyword search. Each search request supports up to five keywords separated with spaces. Excess keywords are ignored. Users can search for all enterprise employees or specify a department (including the sub-department) for the search.
Controlling corporate directory access rights	● Enterprise employees can be classified into different user levels, and information access policies among different user levels can be configured, including inaccessible, public information accessible, and completely accessible. When users search the corporate directory, the search result is displayed based on the access policy. ● This function is configured by the system administrator on the USM-uPortal and synchronized to the CloudECS-BMU.
Sorting departments	On clients, the department tree of the corporate directory is displayed based on the department sorting order specified by the system administrator. This function is configured by the system administrator on the USM-uPortal and synchronized to the CloudECS-BMU. The Desktop Client supports the tree display for the directory while the Mobile Client does not.

Figure 6-9 Tree structure



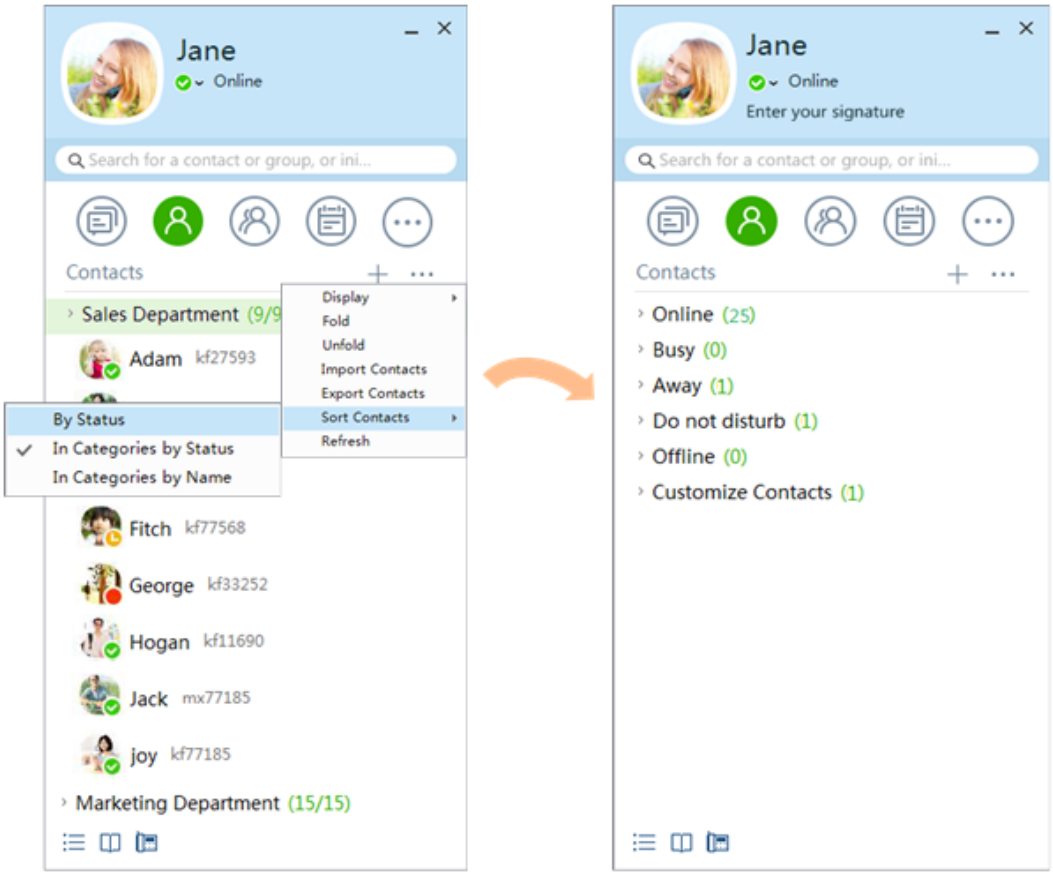
Personal Directory

Contacts in the personal directory for an enterprise user are stored on the CloudECS server. The enterprise user can use personal UC soft clients to access the personal directory.

Function	Description
Managing contact groups	Users can create, delete, and rename groups, add or delete group members, and set the group order (by moving groups up or down). This function is supported only by the Desktop Client.
Managing contacts	Contacts in the personal directory can be divided into two types: customized contacts and enterprise contacts. Customized contacts are those manually created by enterprise users. Enterprise contacts are those searched out in the corporate directory and added to the personal directory. Enterprise contacts are enterprise members. Users can add and delete contacts, modify the nicknames of contacts, and move or copy contacts between groups.
Synchronizing contact information in incremental mode	The system records the modification time stamp of each contact and group. The request for obtaining the personal directory carries the last download time stamp, and the system sends the contact and group information updated after this time stamp to clients. The deleted contacts and groups are marked as deleted.

Function	Description
Displaying a notification when a specified contact goes online	Users can configure the contact online notification function on clients so that users are notified when contacts get online. This function is supported only by the Desktop Client.

Figure 6-10 Managing contacts



6.6 Mobility

The CloudECS supports mobile directory, mobile rich media, and message pushing so that users can experience mobile office on the Mobile Client without location restrictions.

- Mobile directory

  Users can use the Mobile Client to query an enterprise contact in the corporate directory and send a message to or call the contact. This allows users to query colleagues' phone numbers conveniently even if they are not in the office.

- Mobile rich media

  Users can use the Mobile Client to send pictures, voice and video clips, and doodles from their mobile phones. Additionally, they take photos or shoot video clips and send them to other users. This function makes mobile office more diversified, in-time, and

convenient. No matter where they are, users can transfer first-hand information to other users quickly, precisely, and securely.

- Message pushing

  If an IM is received when the Mobile Client is running at the background, the MAA pushes a notification to the mobile phone to ensure that important messages can be delivered in time.

Figure 6-11 Mobile directory

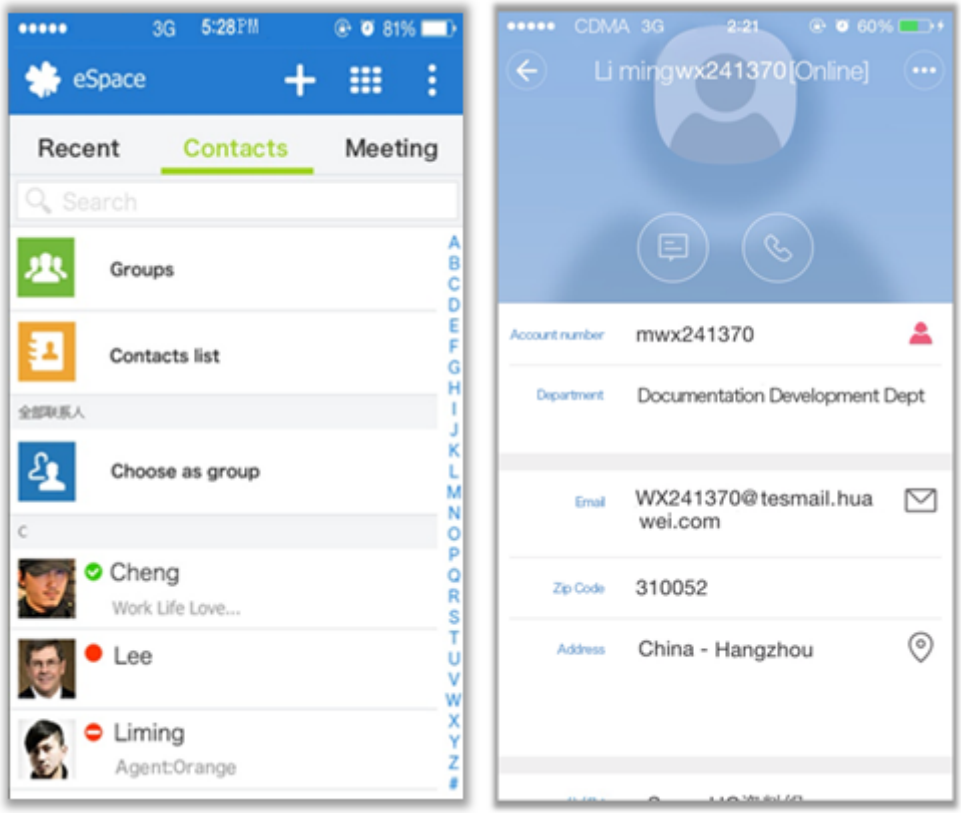
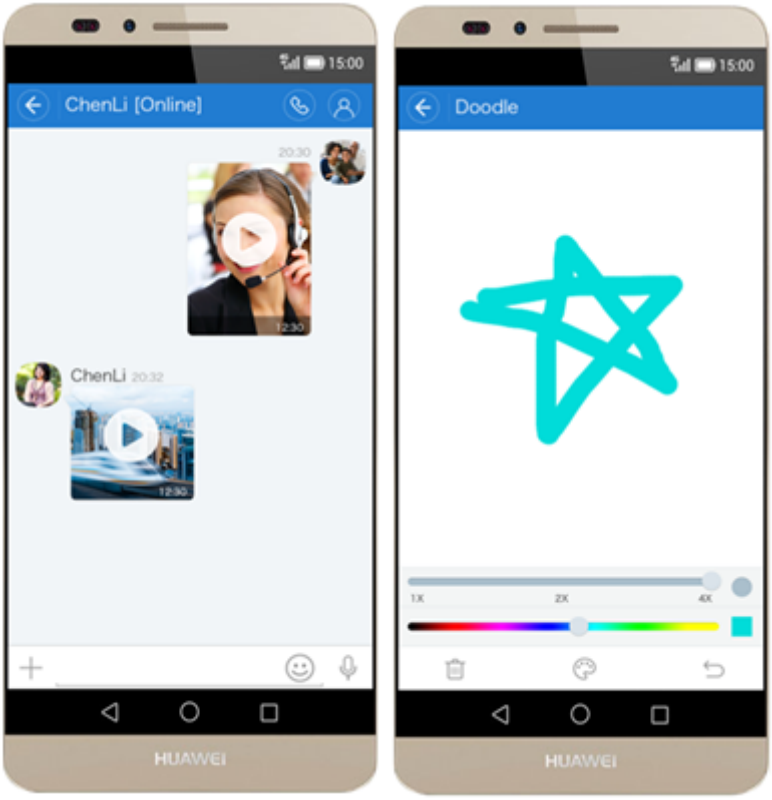


Figure 6-12 Rich media messages



6.7 Work Community

The Work Community is a mobile social networking service based on the Mobile Client. This service provides a brand new content sharing and communication mode for enterprise users. Enterprise users can use their mobile phones to share their work experience and attainments at any time, enhancing the team communication and collaboration efficiency.

Function	Description
Work Community relationship management	● When users use the Work Community for the first time, the system automatically adds bidirectional contacts into the Work Community of each other, and recommends unidirectional contacts in the minimum departments in the recommendation list. Users can select all or some contacts in the list and submit a request for following the Work Community of these contacts. ● After the initial use, users can add or delete Work Community relationships with contacts independently on the contact details screen on the Mobile Client.
Content sharing	● Users can share text, pictures, or video in the Work Community on clients. Text can be sent together with pictures or video. After users share something, their friends can receive red dot notifications and can view the shared contents. ● Users can delete the contents shared by themselves.

Function	Description
Commenting	Users can comment on the contents shared by their friends.
Liking	Users can like the contents shared by their friends.
Picture viewing	Users can tap the profile picture of a friend in the Work Community to view all contents shared by this friend.
Work Community rights management	Users can configure Work Community rights as follows: ● Hide the Work Community to a friend. ● Do not view the Work Community of a friend.

Figure 6-13 Work Community

6.8 Concurrent Online Clients

A user can log in to the Desktop Client and Mobile Client concurrently to send and receive messages. The message records and call records are automatically synchronized between the two clients.

Function	Description
Multi-client login	A user can use the same UC account to log in to the Desktop Client and Mobile Client concurrently. However, the user cannot use the same UC account to log in to the Desktop Client on multiple computers or log in to the Mobile Client on multiple mobile phones concurrently. When a user logs in to the Desktop Client and Mobile Client simultaneously, the VoIP function is available only on the Desktop Client, and the Mobile Client can use only the CTD call mode. The user can log out of the Desktop Client through the Mobile Client so that the VoIP function is available on the Mobile Client.
Multi-client messaging	● When receiving P2P messages or group messages, the system simultaneously delivers the messages to online clients (Desktop Client and Mobile Client) of the recipients. ● When a message is read on one client, the system synchronizes the read state to the other client.
System processing when users are invited to groups	When receiving group invitations, the system delivers the messages to all online clients (Desktop Client and Mobile Client) of the recipients. The system takes the first operation performed on any client as the response.

Figure 6-14 Multi-client concurrent login

7 Reliability

The CloudECS can be deployed in two-node cluster, cluster, or DR mode to ensure service reliability. Each NE can be deployed independently and flexibly.

Two-Node Cluster

The BMU and database can be deployed in two-node clusters in active-active mode and support real-time switchover without service interruption.

Cluster of Three or More Nodes

The eServer, MAA, and UMServer can be deployed in a cluster of up to 11 nodes based on the user capacity requirements, implementing load balancing and improving the system capacity, performance, and reliability.

DR

The CloudECS supports remote DR in active-standby mode. When the system in a location is abnormal due to factors such as natural disasters, the system in another location takes over the services.

8 Security

8.1 Service Security

The CloudECS provides service data encrypted transmission, fine-granularity rights control, and service data access control mechanisms to ensure service security.

Security Technology	Description
Encrypted transmission of service data such as directories and IMs	The CloudECS provides encryption mechanisms and algorithms for the following service interfaces: ● IM interface between UC soft clients and the CloudECS: AES and HMAC-SHA encryption algorithms ● Directory interface between UC soft clients and the CloudECS: AES and HMAC-SHA encryption algorithms ● Rich media and offline file transmission interfaces between UC soft clients and the CloudECS: RSA, AES, and HMAC-SHA encryption algorithms
Message encrypted storage	Historical messages and unread messages can be encrypted for storage in the database and decrypted when read from the database.
User authentication and rights control mechanisms	● Only authenticated users can use services. ● The CloudECS provides the fine-granularity rights control mechanism for each user and user group. ● The CloudECS controls the fine-granularity access rights on all resources of each user. The control operations are performed on the USM-uPortal.

Security Technology	Description
Service data leakage prevention mechanism	● The CloudECS supports configuration of directory information access rights based on the employee level. ● The CloudECS supports keyword filtration of message content to prevent sensitive information transmission in IMs. ● The CloudECS supports filtration based on the file type and file length. ● The CloudECS supports service access control between network areas. That is, IM transmission and file transmission between network areas can be controlled.

8.2 Management Security

The CloudECS provides an independent management plane and supports mainstream security management protocols, strong passwords, and log audit to prevent malicious intrusion and ensure high security of the management layer and the system. The independent management plane is used to separate management data from service data. Service users cannot access the management plane, which reduces the risk for users to access the management plane.

Security Technology	Description
Differentiating service ports from management ports	The CloudECS provides the detailed communication matrix. Enterprise administrators can configure firewall port access policies based on the communication matrix and disable ports that are not in use to reduce intrusion risks.
Comprehensive management protocols	● HTTPS is used for web management. ● FTPS and HTTPS are used for file upload and download. ● Maintenance terminals access the servers through SSH. ● SNMPv3 is used by the NMS to manage service NEs. (provided by the OMU)
Logout upon timeout mechanism	A user will be automatically logged out of the management system when the user is idle for a specified duration.
Audit	The system records operation logs and run logs of different components, and these logs can be viewed and downloaded for further audit. Audit information stored in the system supports strict access control, and only administrators with specified audit rights can view and perform operations on the audit information.

Security Technology	Description
Operating system and database security hardening	● The CloudECS depends on common operating systems (SUSE Linux 11) and databases (Oracle 11g). The latest patches provided by the supplier for common operating systems and databases have been installed when the Huawei CloudEC solution is delivered. ● The CloudECS performs security hardening operations on common operating systems and databases and provides the security hardening guide.
Software integrity verification mechanism	● The CloudECS uses the Secure Hash Algorithm (SHA) to calculate the hash value of each software component. The software component digests are generated and stored in the hash file released with software. ● To prevent the digests from being tampered with, the CloudECS uses the signature tool to sign a digital signature on the hash file and release the signature and hash file with the software package. ● During system software installation, the signature verification tool is used to verify the signature in the hash file.

8.3 Network Security

The CloudEC solution provides a secure network scheme to ensure the IP network security.

The CloudECS meets the following network security principles:

- Service servers and NMS servers need to be deployed in the core server area of the intranet. Firewalls need to be deployed at the egress of the core server area to isolate security domains and control access.
- You are also advised to deploy firewalls at the egress of the maintenance terminal area to control access and focus on protection of terminals on the management plane.
- The proxy access gateway is deployed in the DMZ to process access and service requests sent from extranet users. Firewalls are deployed at the network borders to isolate security zones and control access.

Figure 8-1 Security zone division in the on-premises scenario

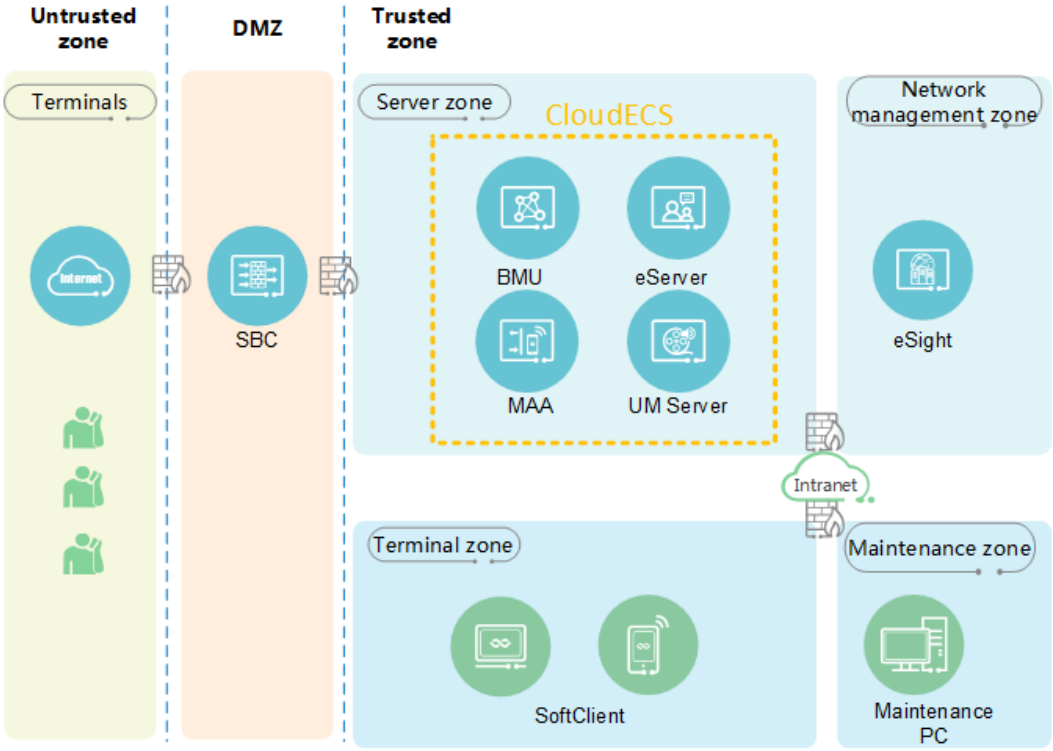
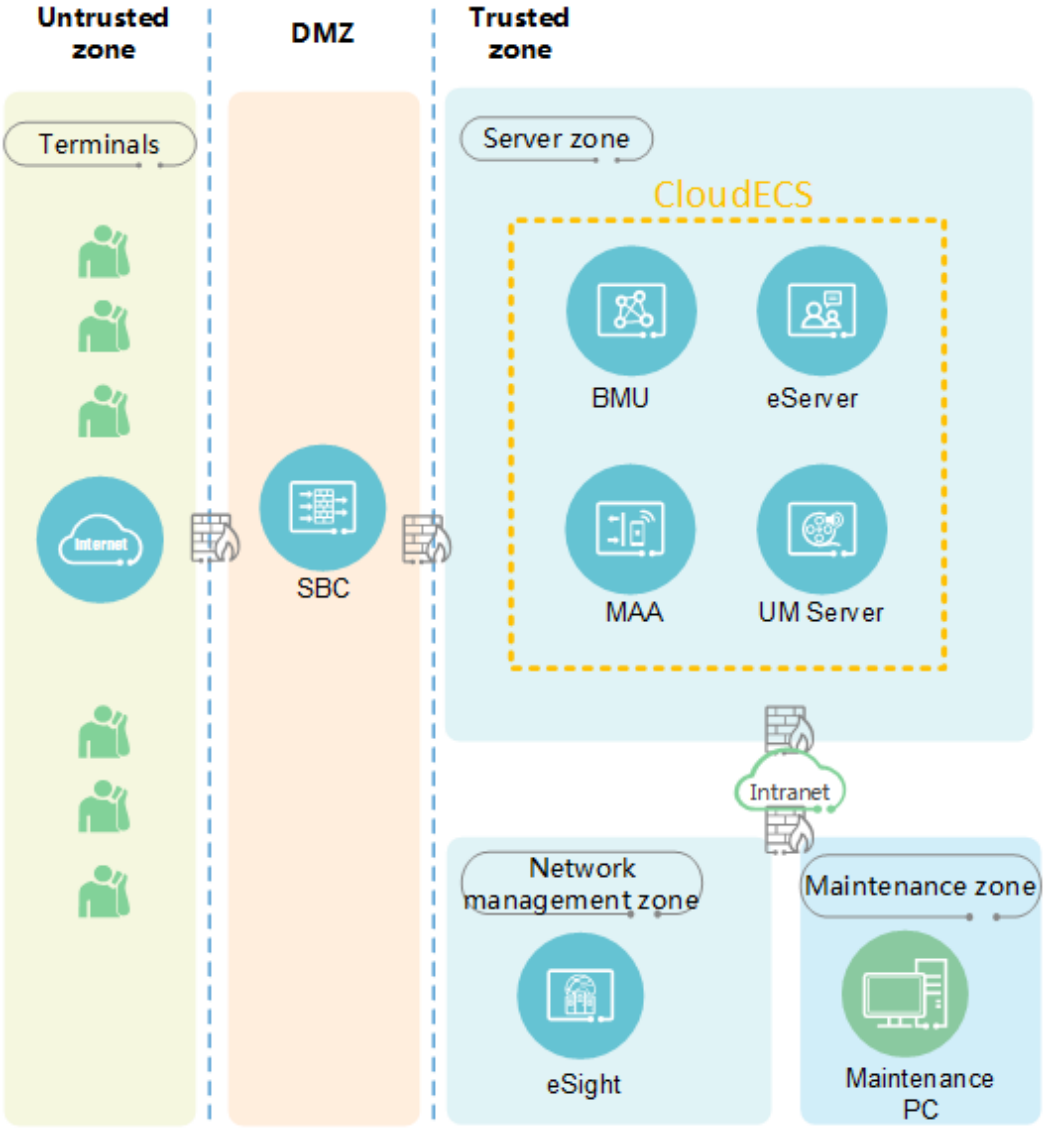


Figure 8-2 Security zone division in the hosted scenario



9 Openness

The CloudECS provides open capabilities for third-party apps through the eSDK server. The supported capabilities include message-, status-, and bulletin-related capabilities, group management, and file delivery.

10 Operation and Maintenance

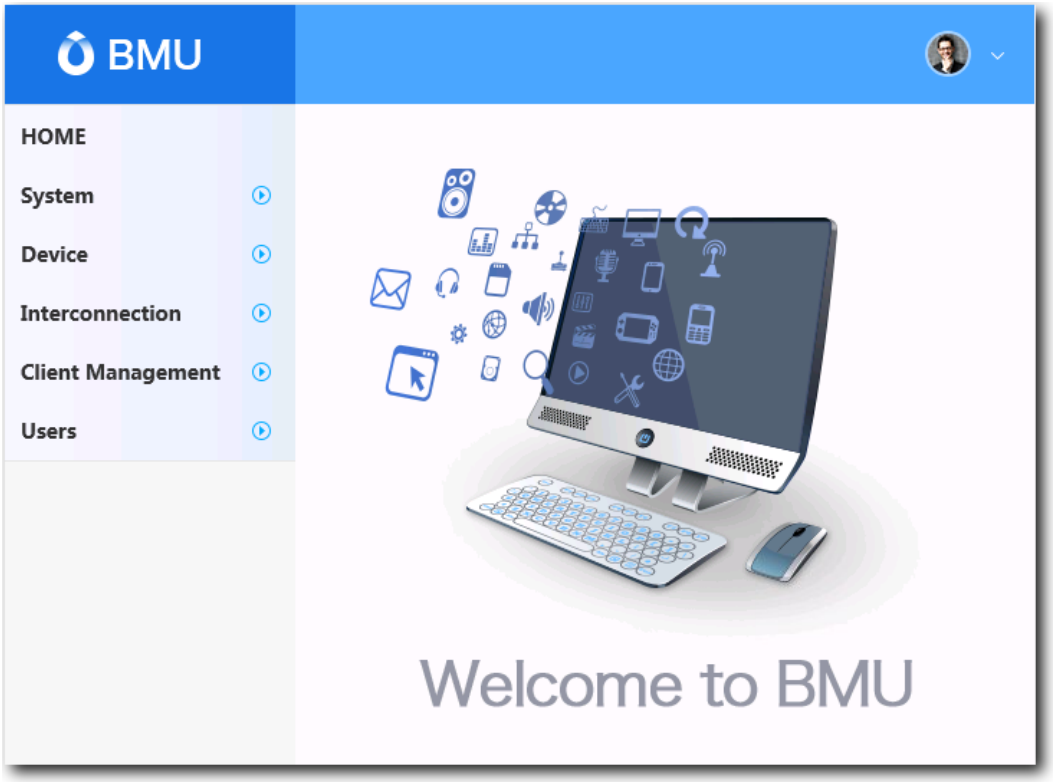
The CloudECS provides the BMU for the system administrator to perform operation and maintenance operations. Additionally, the CloudECS supports unified background maintenance using the operation and maintenance unit (OMU).

The BMU provides a management portal that supports a variety of CloudECS management functions, including Desktop Client and Mobile Client upgrade policy management, CloudECS service parameter management, and management of interworking between CloudECS servers and peripheral NEs.

BMU Function	Description
System management	Provides system-level configuration functions. ● System configuration: supports service, certificate, log, audit, alarm, and authentication configuration. ● License maintenance: allows the system administrator to view license information and upload, export, or revoke the license file. ● Log management: allows the system administrator to view operation and security logs, collect log files of each module, and enable log tracing based on the user account and module. ● MAA parameter maintenance: allows the system administrator to query MAA service parameters, including configuration parameters, values, and description, among which the values can be modified. ● Message tracing: allows the system administrator to trace Representational State Transfer (REST) and WebSocket interface messages. ● Service data backup: allows the system administrator to back up configuration files and database files of the BMU, eServer, UMServer, and MAA to the OMU or a third-party server, and supports manual and automatic backup modes.

BMU Function	Description
Device management	Provides the functions for managing each NE. ● Device maintenance: allows the system administrator to view the CPU, memory, and active/standby status of servers or modules. ● Service maintenance: allows the system administrator to configure UMServer, message, and upgrade service for intranet and extranet areas. ● UMServer: allows the system administrator to view UMServer information, including the IP address, port number, storage path, and disk space usage.
Interworking configuration	● USM interworking: allows the system administrator to configure the interworking with the USM-uPortal. Service provisioning data on the uPortal can be synchronized to the CloudECS only after the interworking is configured. ● Interface open configuration: provides the BMU, AppAgent, and eServer management interfaces and the IP address whitelist for interworking with third-party systems.
Client management	● Area visit maintenance: allows the system administrator to control rights for users in different areas to send IMs, files, and snapshots to each other. ● Client parameters: allows the system administrator to set plug-in parameters, which take effect for UC soft clients globally. ● Desktop Client upgrade: allows the system administrator to upload upgrade packages or patches, configure whether to perform a full upgrade, and specify the installation mode (optional, scheduled, or forcible). ● Mobile Client upgrade: allows the system administrator to create a Mobile Client version and specify the operating system type, version number, upgrade priority, and forcible upgrade option. ● Soft client logs: UC soft clients can upload logs to the UMServer. When permitted by users, technical personnel can collect UC soft client logs through the BMU.
User management	Provides operation statistics on UC users. Account list: allows the system administrator to search for a user based on the account, name, or soft client number and view information such as the account version, recent login IP address, and login time. Online statistics: allows the system administrator to view real-time online user statistics and those in last 24 hours, in last 30 days, and in any specified time segment in charts. Terminal version statistics: allows the system administrator to view the current terminal version proportions and query the terminal version trends in a historical time segment.

Figure 10-1 BMU home page



In addition to the BMU, the system administrator can also use the OMU to maintain the CloudECS.

OMU Function	Description
Version information collection	Allows the system administrator to manually collect CloudECS version information if the Versatile Tools Suite (VTS) tool is not deployed.
Alarm information collection	Allows the system administrator to collect CloudECS alarm information based on the alarm severity and start time.
Event information collection	Allows the system administrator to collect CloudECS event information based on the event type and start time.
System resource status collection	Allows the system administrator to collect status information about system resources such as the module timer, message package, and memory partition to learn the system running status in a timely manner.
License information collection	Allows the system administrator to run a command to query the actual usage of the CloudECS license.

OMU Function	Description
Man-machine language (MML) configuration information collection	Allows the system administrator to collect MML configuration information about the CloudECS to learn the NE configuration and therefore further analyze fault sources.
NE operation and run log collection	Allows the system administrator to collect NE operation and run logs. Operation logs record operations that are performed on NEs recently and help analysis of fault sources. Run logs record running information about each process, including exception information, which can be used in troubleshooting and cause analysis.
Virtual machine (VM) management	Allows the system administrator to add, delete, modify, query, reset, stop, start, and format VMs.
Process management	Allows the system administrator to start, stop, and restart processes and query the process status of each module.
Office information management	Allows the system administrator to query and change the IP addresses of the BMU, eServer, MAA, and UMServer.
Database management	Allows the system administrator to change the database IP address and password.

Figure 10-2 OMU web management page

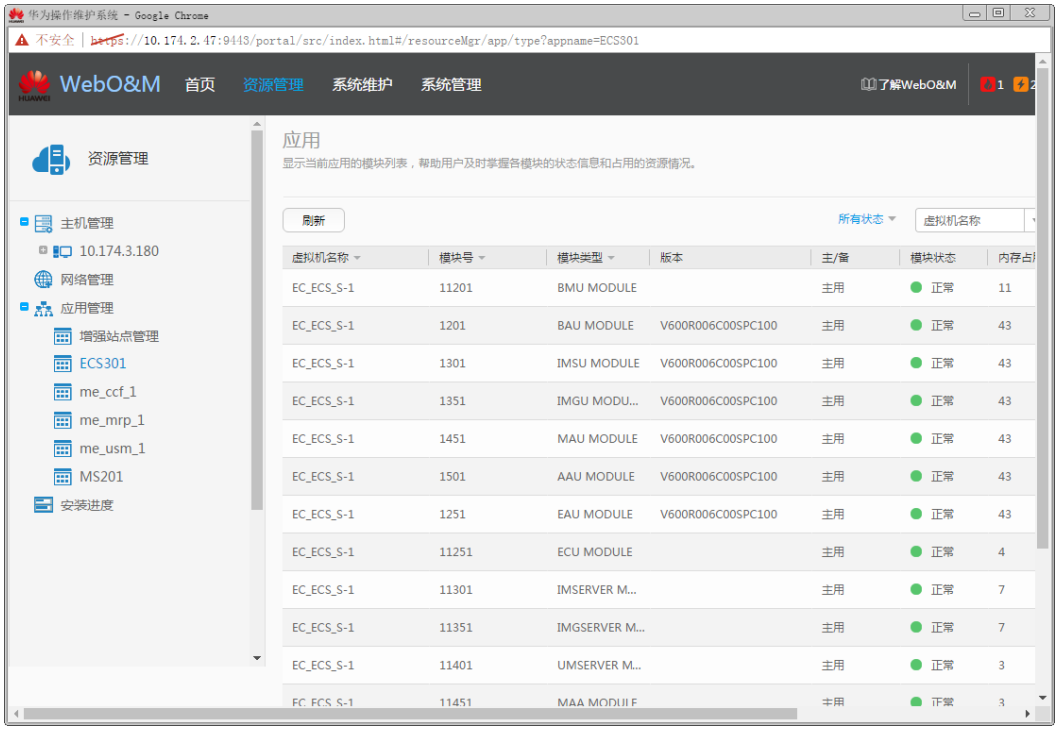
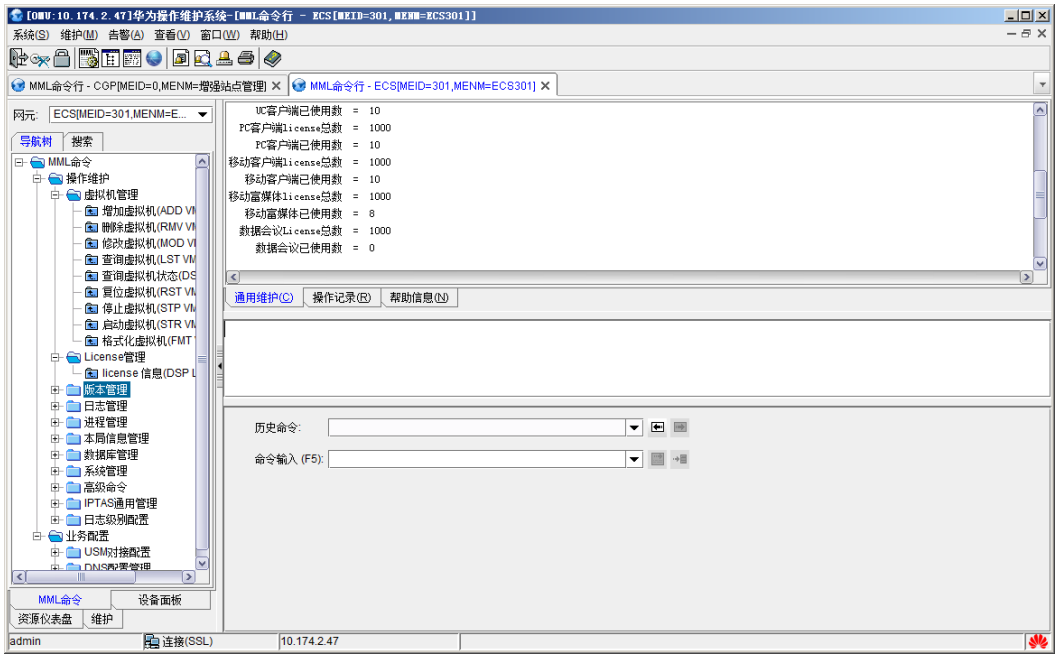


Figure 10-3 OMU client



11 Technical Specifications

NOTE

The number of users/devices refers to the maximum number of users if users use only the Desktop Client, and refers to the maximum number of devices if users may use the Desktop Client and Mobile Client concurrently.

Category	Item	0 ≤ Number of Users/ Devices < 2000	2000 ≤ Number of Users/ Devices < 10,000	10,000 ≤ Number of Users/ Devices < 40,000	40,000 ≤ Number of Users/ Devices < 400,000	Remarks
Resource usage	Average CPU usage	<70%	< 70%	< 70%	< 70%	Indicates the average resource usage when all users are online.
	Average memory usage	<70%	< 70%	< 70%	< 70%	
Mobile capacity	Maximum percentage of Mobile Client users	30%	30%	30%	30%	Indicates the maximum percentage of users who can log in to the Mobile Client. To support a higher percentage, you need to plan more nodes for the multi-node MAA cluster.

Category	Item	0 ≤ Number of Users/ Devices < 2000	2000 ≤ Number of Users/ Devices < 10,000	10,000 ≤ Number of Users/ Devices < 40,000	40,000 ≤ Number of Users/ Devices < 400,000	Remarks
	Maximum percentage of users who use the Desktop Client and Mobile Client concurrently	10%	10%	10%	10%	Indicates the maximum percentage of users who can log in to the Desktop Client and Mobile Client concurrently.
Login performance	Centralized login duration (in minutes)	10	10	15	60	Indicates the maximum duration required for all users to log in to clients in a centralized manner.
	Maximum login CAPS	32	32	64	128	-
	Maximum mobile login CAPS (single MAA)	4	4	8	8	-
Message specifications	Maximum downlink text message CAPS	50	50	200	2000	Includes all downlink messages such as P2P and group downlink messages.
	Maximum CAPS for message interfaces provided for the eSDK	50	50	200	2000	-
	Unread message reading CAPS	32	32	64	128	-
	Historical message obtaining CAPS	5	5	20	200	-

Category	Item	0 ≤ Number of Users/ Devices < 2000	2000 ≤ Number of Users/ Devices < 10,000	10,000 ≤ Number of Users/ Devices < 40,000	40,000 ≤ Number of Users/ Devices < 400,000	Remarks
Presence specifications	Maximum status release CAPS	15	15	60	600	-
Group specifications	Maximum number of contact groups	2000	100,000	400,000	4,000,000	-
	Maximum number of members per contact group	500	500	500	500	-
	Maximum number of temporary groups	4000	200,000	800,000	8,000,000	-
	Maximum number of members per temporary group	100	100	100	100	-
Corporate directory specifications	Maximum number of user records in the corporate directory	5000	30,000	120,000	800,000	-
	Maximum corporate directory query CAPS from soft clients	5	5	20	200	-
Rich media specifications	Maximum number of concurrent connections supported by a single UMServer (1:4 upload-to-download ratio)	40	40	150	150	-

Category	Item	0 ≤ Number of Users/ Devices < 2000	2000 ≤ Number of Users/ Devices < 10,000	10,000 ≤ Number of Users/ Devices < 40,000	40,000 ≤ Number of Users/ Devices < 400,000	Remarks
	Maximum bandwidth for a single UMServer (in MB/s)	15	15	75	75	-
ECS hosted multi-tenant specifications	Maximum number of tenants	N/A	10,000			-
	Maximum number of PGM users	N/A	400,000			-
	Maximum number of PGM devices	N/A	400,000			-
	Maximum number of devices for a single tenant	N/A	(0, 400000]			-