Huawei Qiankun

MSP Operation Guide

Issue	01
Date	2023-04-30

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://www.huawei.com

Email: support@huawei.com

Contents

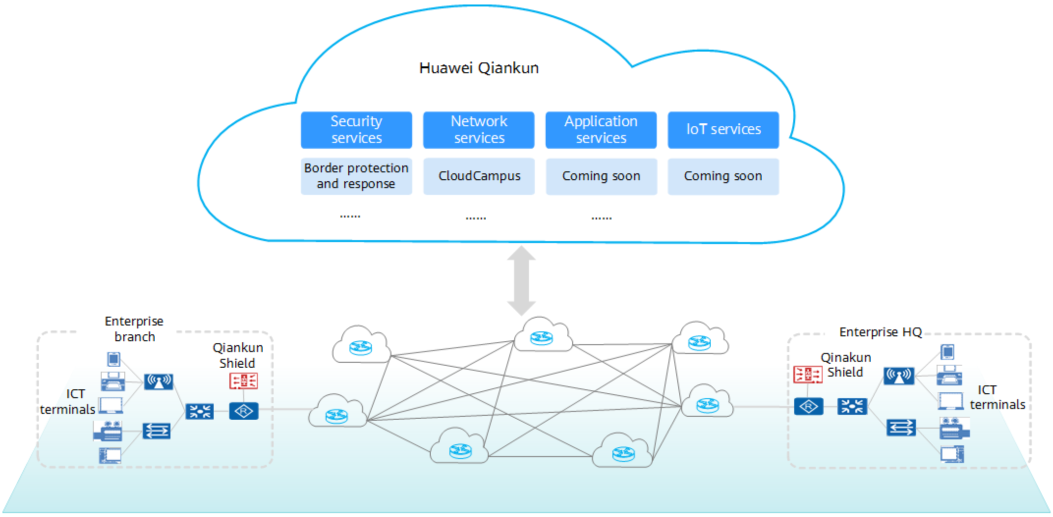
1 Service Introduction

Overview

Huawei Qiankun is a collection of one-stop digital network cloud services, covering network management, security, and connection, helping enterprises simplify and secure their networks. Figure 1-1 shows the architecture of Huawei Qiankun.

The conventional offline procurement and deployment mode has disadvantages in long procurement period and slow function update. Huawei Qiankun addresses these issues by offering e-commerce-style self-service procurement, pay-per-use high-quality services, and elastic scaling capabilities to enterprises.

Figure 1-1 Architecture of Huawei Qiankun



Benefits

As enterprises have an increasing number of branches and a more variety of devices and are faced with more security threats, they have strong demands for unified network management and control, unified operations and maintenance (O&M), and unified security event handling. Huawei Qiankun meets all these requirements by providing integrated "cloud-network-device" management and control. Table 1-1 lists the benefits of Huawei Qiankun.

Table 1-1 Benefits of Huawei Qiankun

Customer Requirement	Benefit of Huawei Qiankun
Fast deployment, professional and unified cloud-based network O&M	Supports automated network deployment and orchestration, barcode scanning–based deployment, intelligent verification, cloud-based network inspection, and health monitoring, greatly simplifying O&M.
Professional security O&M, security standards compliance	Automatically handles security events on the cloud, provides the 24/7 cloud-based security expert service, and offers a one-stop security standards compliance package.
Application experience assurance and optimization	Provides application visualization and assurance services, such as 3D Wi-Fi simulation and network dashboards, to improve application experience.
Unified management of Internet of Things (IoT) terminals, such as cameras, sensors, and electric meters	Provides IoT awareness and security services to enable fast network access, unified O&M, and security risk monitoring for IoT terminals.

2 MSP Introduction

Basic Concepts

Target user groups of Huawei Qiankun include tenants and managed service providers (MSPs).

- Tenants are enterprise users or organizations that purchase cloud services and devices to meet their business development requirements.
- MSPs are organizations with professional service management and maintenance capabilities. They provide network deployment, management, security detection, security protection, and O&M for tenants.

  NOTE

  An MSP in the cyber security field is called a managed security service provider (MSSP).

Responsibilities of MSPs

- For tenants:

  MSPs can provide comprehensive network construction, service management, and security O&M for tenants who entrust the MSPs with services of Huawei Qiankun. This helps tenants reduce their operational expenditure (OPEX).
- For Huawei Qiankun operations personnel:

  Huawei Qiankun operations personnel are responsible for new user attraction and activeness promotion.

  MSPs, as important partners of the Huawei Qiankun operations team, offer assistance to its product promotion and selling.

  Therefore, MSPs are often referred to as Huawei Qiankun agents.

MSPs, tenants, and Huawei Qiankun operations personnel are closely related to each other. For details about their relationships and respective responsibilities, see **Table 2-1**.

Table 2-1 Responsibilities of users and relationships between them

User Category	User Creation	Major Responsibilities
Tenant	● Self-registration ● Created by MSP administrators	Responsibilities of tenants vary according to their IT capabilities. ● Tenant-managed construction and maintenance: Tenant administrators complete device onboarding, network deployment, and service O&M by themselves. ● MSP-managed construction and maintenance: Tenant administrators entrust MSPs with network construction and maintenance.
MSP	● Qualified and created by Huawei Qiankun operations personnel	● MSP-managed construction: MSPs complete device onboarding and network deployment for tenants. ● MSP-managed maintenance: After tenants entrust services to MSPs, the MSPs perform routine monitoring and periodic inspection on the services, handle exceptions and issues found during service running, and provide risk assessment and event handling suggestions. ● Promotion and selling of Huawei Qiankun **NOTE** Some services, such as the Border Protection and Response Service, can be purchased offline through MSPs. For details, see the corresponding service documents.
Huawei Qiankun operations personnel	Self-creation upon installation of the Huawei Qiankun platform	● Marketing activities of Huawei Qiankun: new user attraction and activeness promotion ● Management and creation of MSP accounts

3 MSP Account Types

Account Introduction

MSP-managed construction and maintenance are mainly carried out on the Huawei Qiankun console.

Currently, the console supports tenant accounts and MSP accounts. The relationship between the two is as follows:

- A tenant account can establish agency relationships with multiple MSP accounts.
- An MSP account can manage services of multiple tenant accounts.

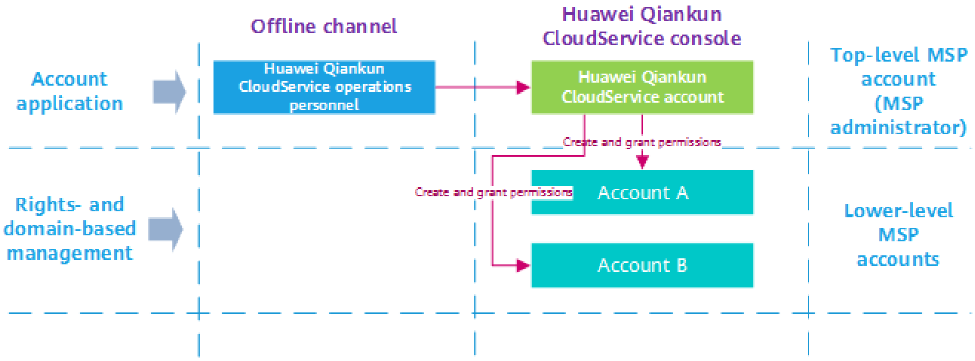
MSP Account Types

As shown in **Figure 3-1**, the first account created for an MSP has all operation permissions and is therefore known a top-level MSP account.

A top-level MSP account can create lower-level MSP accounts and grant permissions to these accounts.

For details about how to grant permissions to lower-level MSP accounts, see **8 MSP Account Management**.

Figure 3-1 MSP account types

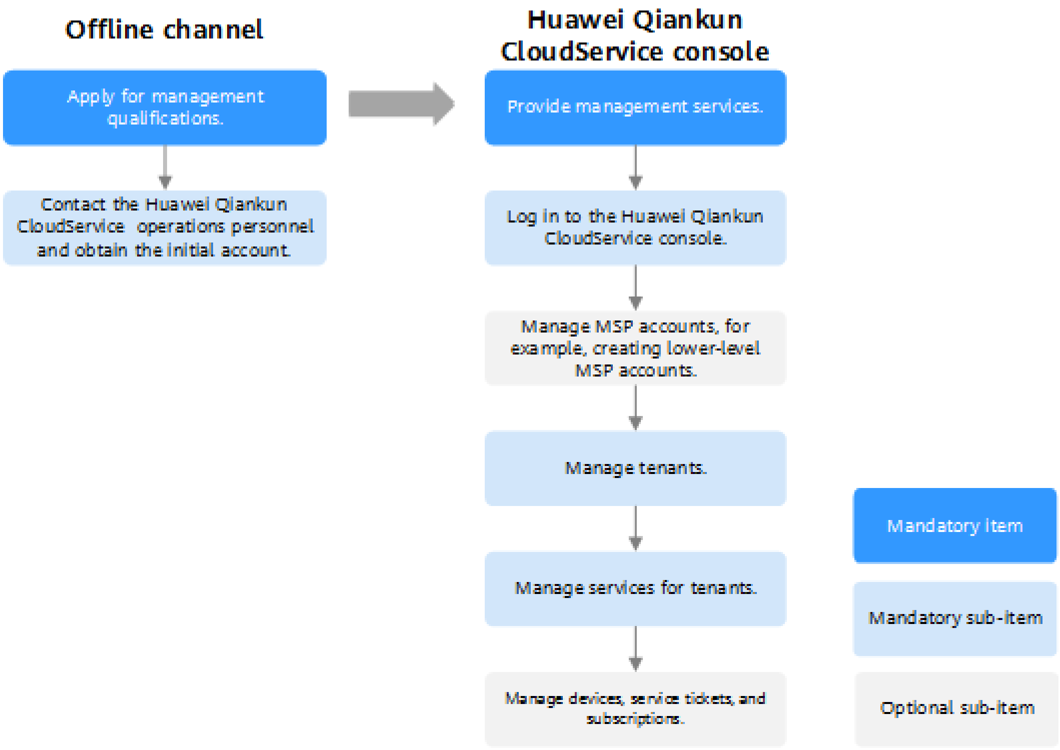

Offline channel
Huawei Qiankun CloudService console
Account application
Huawei Qiankun CloudService operations personnel
Huawei Qiankun CloudService account
Top-level MSP account (MSP administrator)
Create and grant permissions
Create and grant permissions
Rights- and domain-based management
Account A
Account B
Lower-level MSP accounts

Service Use Process

The process of using Huawei Qiankun through an MSP account involves two stages: applying for management qualifications and providing management, as shown in **Figure 3-2**.

1. Applying for management qualifications: Contact Huawei Qiankun operations personnel at **sa@huawei.com**, provide related materials, and obtain the initial account after the application is approved.
2. Providing management: Log in to the Huawei Qiankun console and perform routine management and maintenance on services entrusted by tenants.

Figure 3-2 Service use process


Offline channel
Apply for management qualifications.
Contact the Huawei Qiankun CloudService operations personnel and obtain the initial account.
Huawei Qiankun CloudService console
Provide management services.
Log in to the Huawei Qiankun CloudService console.
Manage MSP accounts, for example, creating lower-level MSP accounts.
Manage tenants.
Manage services for tenants.
Manage devices, service tickets, and subscriptions.
Mandatory item
Mandatory sub-item
Optional sub-item

NOTE

This document describes the overall process and common operations of using Huawei Qiankun through an MSP account. For details about how to use an MSP account to manage a specific service for a tenant, see the user guide of this service.

4 Account Registration and Login to the Console

Context

The Huawei Qiankun console is mainly used for service configuration and management. Before logging in to the Huawei Qiankun console, register an account first.

Procedure

Step 1 Register a Huawei Qiankun account.

NOTE

Currently, MSPs cannot register Huawei Qiankun accounts by themselves.

To become an agent of Huawei Qiankun, contact the operations personnel at **sa@huawei.com** to apply for the MSP qualification.

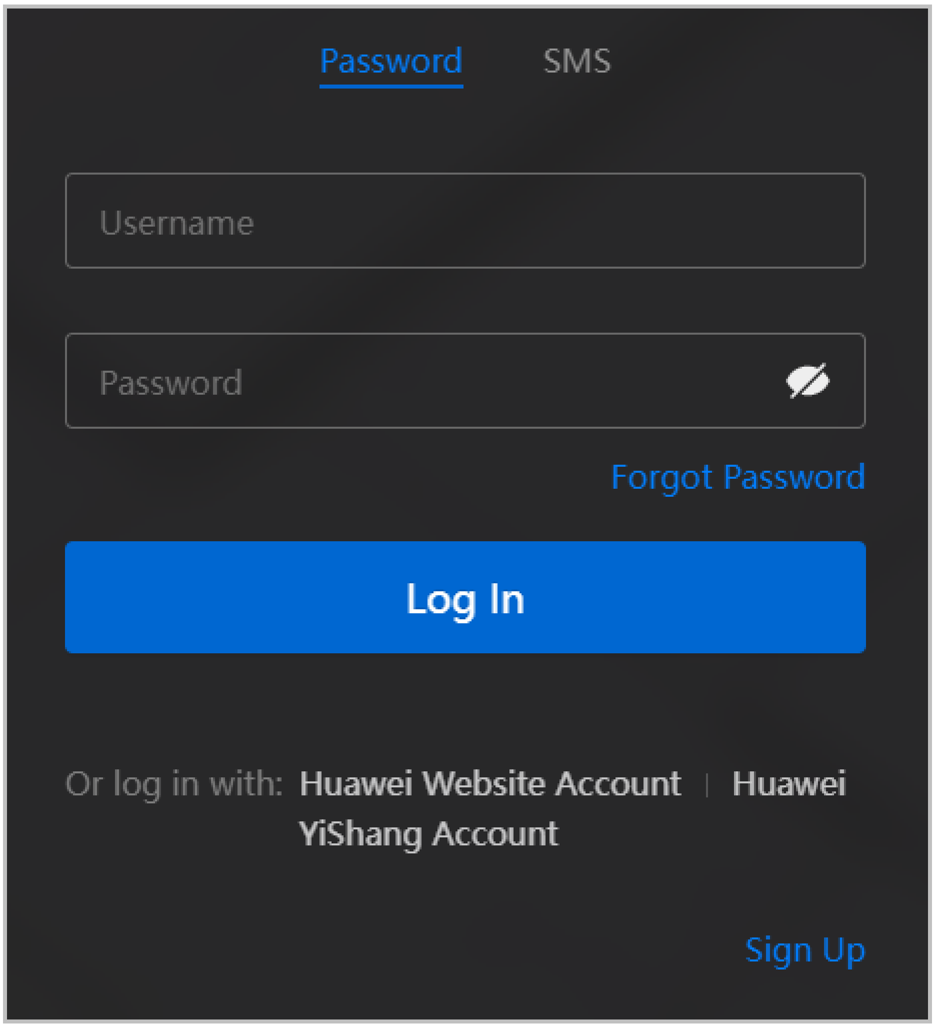
After successful qualification approval, Huawei Qiankun operations personnel will create an MSP account for you.

Step 2 Use the MSP account created by the operations personnel to log in to the Huawei Qiankun **console**.

⚠ CAUTION

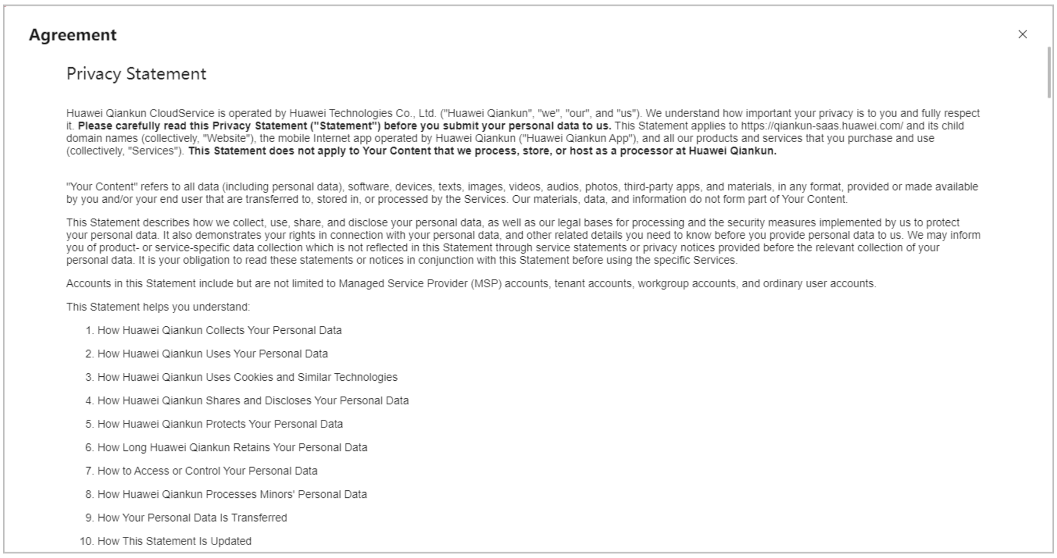
- Keep the username and password of your Huawei Qiankun account safe.
- If you fail to log in for five consecutive times, the system automatically locks your account for 10 minutes.

Figure 4-1 Console login page


Password
SMS
Username
Password
Forgot Password
Log In
Or log in with: Huawei Website Account | Huawei YiShang Account
Sign Up

Step 3 In the case of the first login, read the privacy statement and customer agreement carefully, and click **I Have Read and Agree to the Content**.

Figure 4-2 Signing agreements



Agreement

Privacy Statement

Huawei Qiankun CloudService is operated by Huawei Technologies Co., Ltd. ("Huawei Qiankun", "we", "our", and "us"). We understand how important your privacy is to you and fully respect it. **Please carefully read this Privacy Statement ("Statement") before you submit your personal data to us.** This Statement applies to https://qiankun-saas.huawei.com/ and its child domain names (collectively, "Website"), the mobile Internet app operated by Huawei Qiankun ("Huawei Qiankun App"), and all our products and services that you purchase and use (collectively, "Services"). **This Statement does not apply to Your Content that we process, store, or host as a processor at Huawei Qiankun.**

"Your Content" refers to all data (including personal data), software, devices, texts, images, videos, audios, photos, third-party apps, and materials, in any format, provided or made available by you and/or your end user that are transferred to, stored in, or processed by the Services. Our materials, data, and information do not form part of Your Content.

This Statement describes how we collect, use, share, and disclose your personal data, as well as our legal bases for processing and the security measures implemented by us to protect your personal data. It also demonstrates your rights in connection with your personal data, and other related details you need to know before you provide personal data to us. We may inform you of product- or service-specific data collection which is not reflected in this Statement through service statements or privacy notices provided before the relevant collection of your personal data. It is your obligation to read these statements or notices in conjunction with this Statement before using the specific Services.

Accounts in this Statement include but are not limited to Managed Service Provider (MSP) accounts, tenant accounts, workgroup accounts, and ordinary user accounts.

This Statement helps you understand:

1. How Huawei Qiankun Collects Your Personal Data
2. How Huawei Qiankun Uses Your Personal Data
3. How Huawei Qiankun Uses Cookies and Similar Technologies
4. How Huawei Qiankun Shares and Discloses Your Personal Data
5. How Huawei Qiankun Protects Your Personal Data
6. How Long Huawei Qiankun Retains Your Personal Data
7. How to Access or Control Your Personal Data
8. How Huawei Qiankun Processes Minors' Personal Data
9. How Your Personal Data Is Transferred
10. How This Statement Is Updated

Step 4 In the case of the first login, the system prompts you to change your password. For account security purposes, change the initial password immediately.

📖 **NOTE**

The password requirements are as follows:

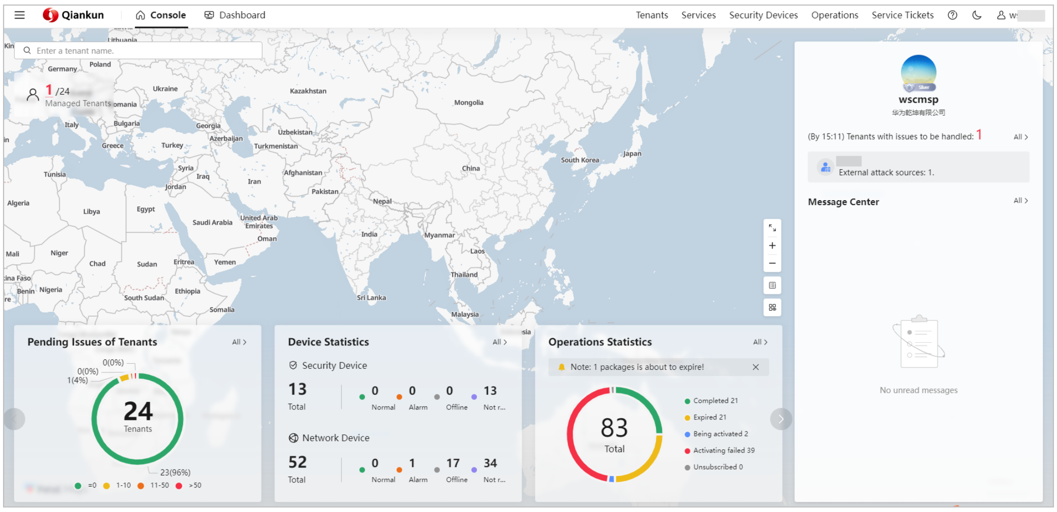
- The password is a string of 8 to 32 characters.
- The password contains at least one letter and one digit.
- The password does not contain sensitive information, such as your username, phone number, and email address.
- Common and weak passwords are not recommended.

----End

5 MSP Homepage

The MSP homepage consists of four modules. For details about these modules, refer to **Table 5-1**.

Figure 5-1 MSP homepage



(By 15:11) Tenants with issues to be handled: 1

External attack sources: 1.

Note: 1 packages is about to expire!

No unread messages

Table 5-1 Introduction to the MSP homepage

Module		Description
Menu bar	--	Displays items such as **Tenants**, **Services**, **Security Devices**, **Operations**, and the account, as well as the managed service list and dashboard entry on the left. ● You can click the Huawei Qiankun logo on the left to redirect to Huawei Qiankun Marketplace. ● Click **Console** to go to the Huawei Qiankun console homepage.

Module		Description
Map	--	Displays the locations of existing managed tenants. ● Enter the name of a tenant in the search box in the upper left corner of the map, and click 🔍 or press **Enter** to search for the tenant. You can click **Enter Management View** or **Locate** in the **Operation** column of a tenant. ● View the total number of managed tenants and abnormal managed tenants in the upper left corner of the map. You can click 👤 to go to the **Managed Tenants** page. ● Click a tenant icon to view the tenant information in detail. On the **Tenant Detail** page that is displayed, you can click **Enter Management View** and view the pending events of the tenant. ● Move the cursor to a tenant icon. On the displayed page, you can click **Change Location** to change the location of the tenant or **Enter Management View** to manage services of the tenant. **NOTE** ● The map is displayed in auto mode by default. You can click ▦ in the lower right corner of the map, select **Custom Mode**, and click **Save** to change the map view mode. Then click **Save**. ● Click ⤢ in the menu bar to display the map in full screen. ● To zoom in or out the map, move the scroll wheel, click an aggregated site icon, or click **+** or **-** in the lower right corner of the map.
Overview (Click > to swipe the remaining modules from left or right.)	**Pending Issues of Tenants**	Displays the number of pending events of existing tenants. Click **All** to view the tenant information. For details, see **11 Tenant Service Management**.
	Device Statistics	Displays the overall statistics of existing security and network devices. Click **All** to view the security device information. For details, see **12.1 Managing Security Devices**.
	Operations Statistics	Displays the number of packages in each state. Click **All** to view the package information. For details, see **14 Package Management**.

Module		Description
	Service Ticket Statistics	Displays the overview of existing service tickets. Click **All** to view the service ticket information. For details, see **13 Service Ticket Management**. You can click the number under a service ticket status to quickly locate all the service tickets in this status.
	Service Statistics (Top 5 Tenants)	Displays the top five managed tenant services. Click **All** to view the managed tenant service information. For details, see **Service Management**.
	Top 5 Tenants	Displays the top five tenants with the highest number of pending events. You can click a tenant name to view its pending events in detail. ● Click **All** to view the information about all tenants with pending events. For details, see **11 Tenant Service Management**. ● Click a tenant name to view its pending events.
Smart Assistant	--	Displays the pending events of existing tenants. ● Click a pending tenant event to view the event details and handle the event.
Message Center	--	Manages messages in a unified manner. You can click **All** in the upper right corner to access the message center.

6 MSP Dashboard

Prerequisites

You have logged in to the Huawei Qiankun console and have the Border Protection and Response Service permissions.

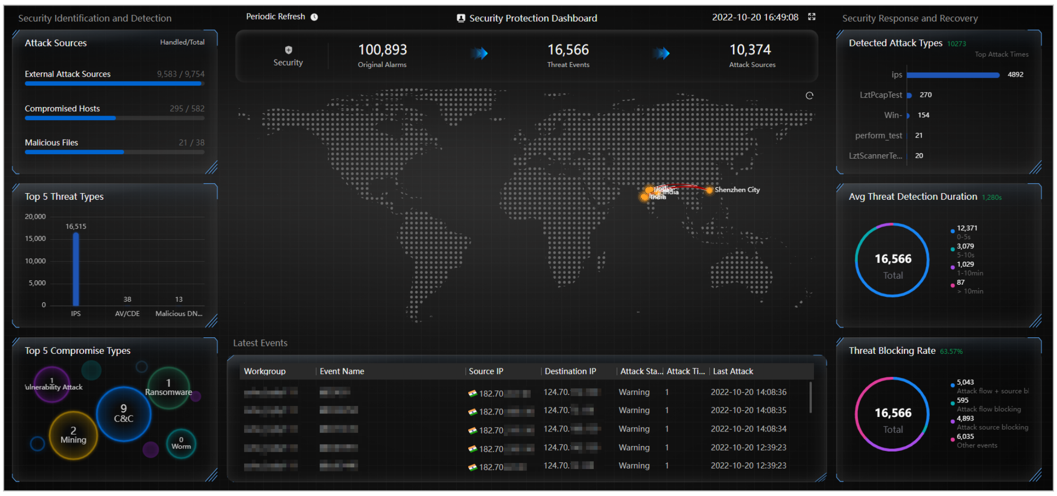
Context

The MSP dashboard consists of three modules: **Security Identification and Detection**, **Latest Events**, and **Security Response and Recovery**. For details about these tables, refer to **Table 6-1**.

Procedure

1. Click **Dashboard** in the upper left corner of the console to access the **Dashboard** page and view the overall security situation.

Figure 6-1 MSP dashboard



Latest Events

Workgroup	Event Name	Source IP	Destination IP	Attack Sta...	Attack Ti...	Last Attack
[redacted]	[redacted]	182.70[redacted]	124.70.[redacted]	Warning	1	2022-10-20 14:08:36
[redacted]	[redacted]	182.70[redacted]	124.70.[redacted]	Warning	1	2022-10-20 14:08:35
[redacted]	[redacted]	182.70[redacted]	124.70.[redacted]	Warning	1	2022-10-20 14:08:34
[redacted]	[redacted]	182.70[redacted]	124.70.[redacted]	Warning	1	2022-10-20 12:39:23
[redacted]	[redacted]	182.70[redacted]	124.70.[redacted]	Warning	1	2022-10-20 12:39:23

Table 6-1 Description of dashboard modules

Module		Description
Security Identification and Detection	Attack Sources	Displays the numbers of handled and total external attack sources, compromised hosts, and malicious files.
	Top 5 Threat Types	Displays top 5 threat event types.
	Top 5 Compromise Types	Displays top 5 compromised host types.
--	Latest Events	Displays threat event information in reverse chronological order.
Security Response and Recovery	Detected Attack Types	Displays top 5 detected attack types.
	Avg Threat Detection Duration	Displays the average time taken by the Huawei Qiankun CloudService platform to detect threat events based on the logs reported by Qiankun Shield devices.
	Threat Blocking Rate	Displays information about threat event blocking. ● **Attack flow + source blocking**: displays the number of threat events that are detected and blocked by security protection policies of Qiankun Shield devices and for which blocklists are delivered. ● **Attack flow blocking**: displays the number of threat events detected and blocked by security protection policies of Qiankun Shield devices. ● **Attack source blocking**: displays the number of threat events for which blocklists are delivered. ● **Other events**: displays the number of threat events that have not been handled yet.

2. View the overall security situation of tenants displayed by label.

   On the **Dashboard** page, click ▼ next to **Filter by Label**, select a label, and view the overall security situation of tenants filtered by the label. For details about how to add a tenant label, see **Tenant Management > Adding a Label**.

7 Personal Center

Personal Information Settings

1. Log in to the console, click your account in the upper right corner, and click **Personal Center**.

   NOTE

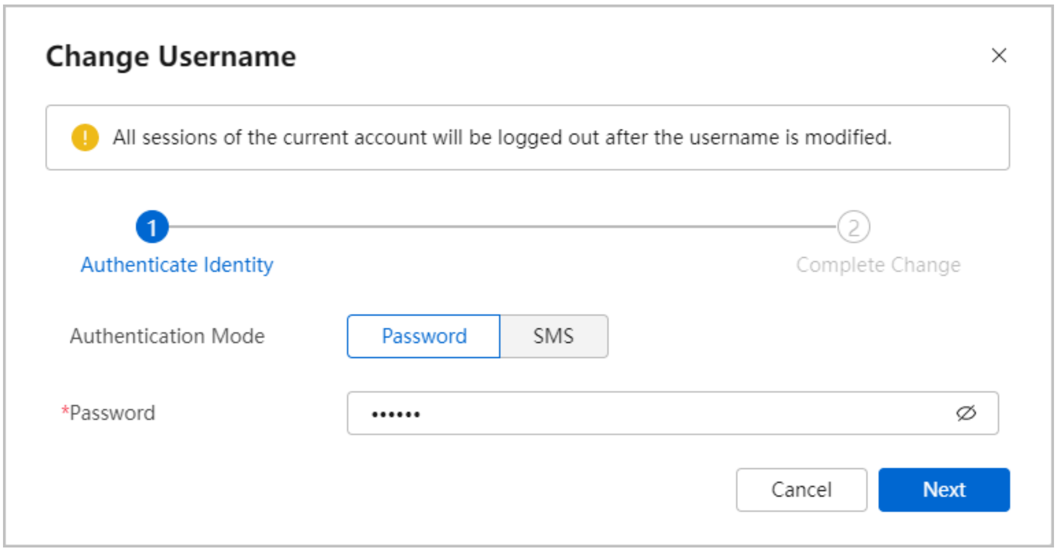
   If an MSP account is authenticated, an authentication identifier is displayed next to the account name on the console.

2. In the **Personal Information** area, click **Upload** next to **Profile Picture**, and select a local image with a size no more than 10 MB.
3. Change the username.

   a. Click ✎ on the right of the username.

   b. In the **Change Username** dialog box, enter your password or a verification code for identity verification, and click **Next**.

   Figure 7-1 Verifying the identity



Change Username

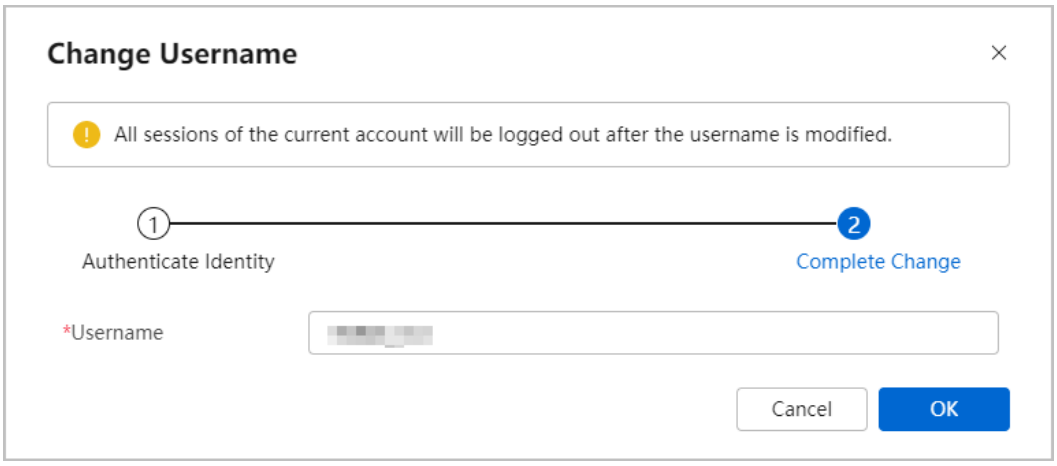
All sessions of the current account will be logged out after the username is modified.

Authentication Mode: Password

*Password: ••••••

   c. After successful verification, enter a new username and click **OK**. Then, use the new username to log in again.

Figure 7-2 Changing the username



Change Username

All sessions of the current account will be logged out after the username is modified.

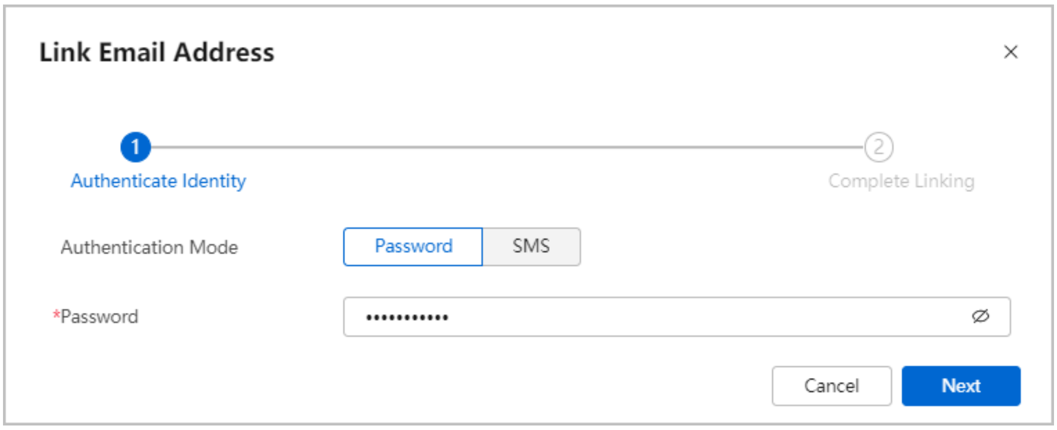
*Username

4. Link a phone number or email address to your current account, in order to receive various notifications (such as service ticket notifications) and verification codes (for example, for password retrieval).

   The following describes how to link an email address. The process of linking a phone number is similar.

   a. Click 🔗 on the right of **Email Address**.
   b. In the **Link Email Address** dialog box, enter your password or a verification code for identity verification, and click **Next**.

Figure 7-3 Verifying the identity



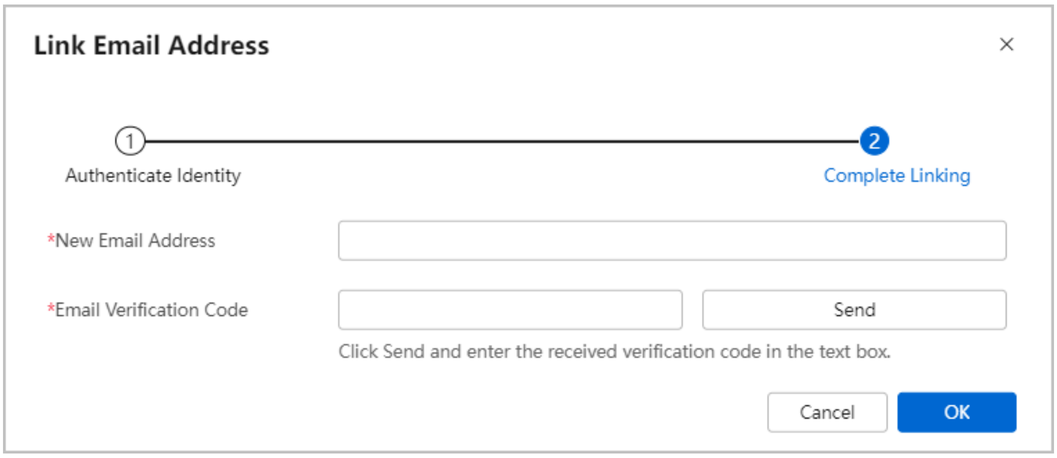
Link Email Address

Authentication Mode: Password | SMS

*Password: •••••••••••

   c. After successful verification, enter an email address and click **OK**.

Figure 7-4 Linking an email address



Link Email Address

Authenticate Identity — Complete Linking

*New Email Address

*Email Verification Code

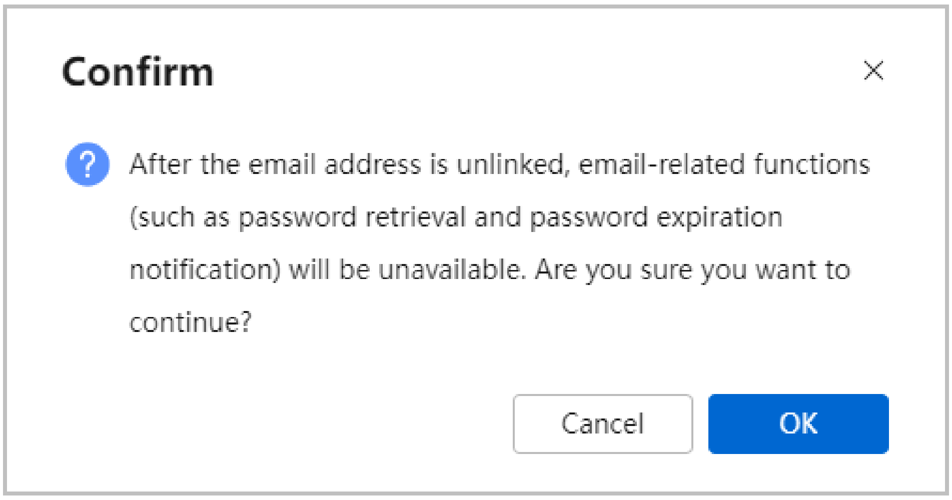
Click Send and enter the received verification code in the text box.

To unlink the email address, do as follows:

a. Click on the right of the linked email address.

b. In the **Confirm** dialog box, click **OK**.

Figure 7-5 Confirm dialog box

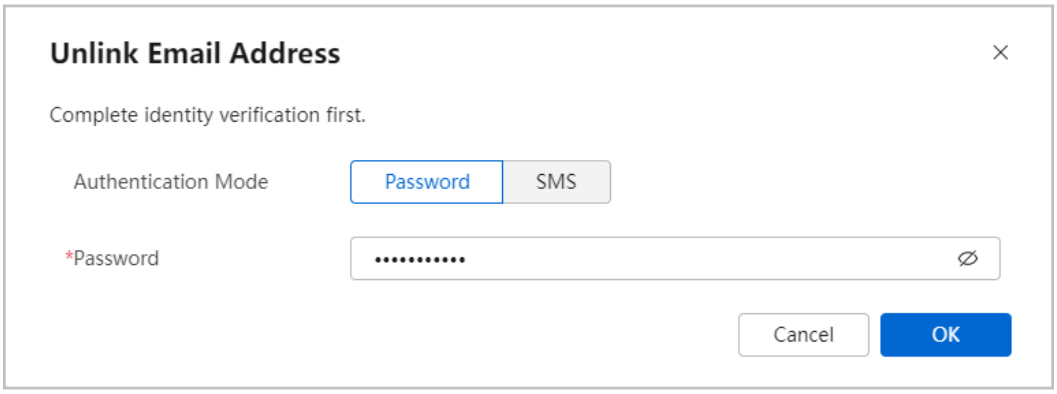


Confirm

After the email address is unlinked, email-related functions (such as password retrieval and password expiration notification) will be unavailable. Are you sure you want to continue?

c. In the **Unlink Email Address** dialog box, enter your password or a verification code for identity verification, and click **OK**.

Figure 7-6 Unlinking the email address



Unlink Email Address

Complete identity verification first.

Authentication Mode: Password | SMS

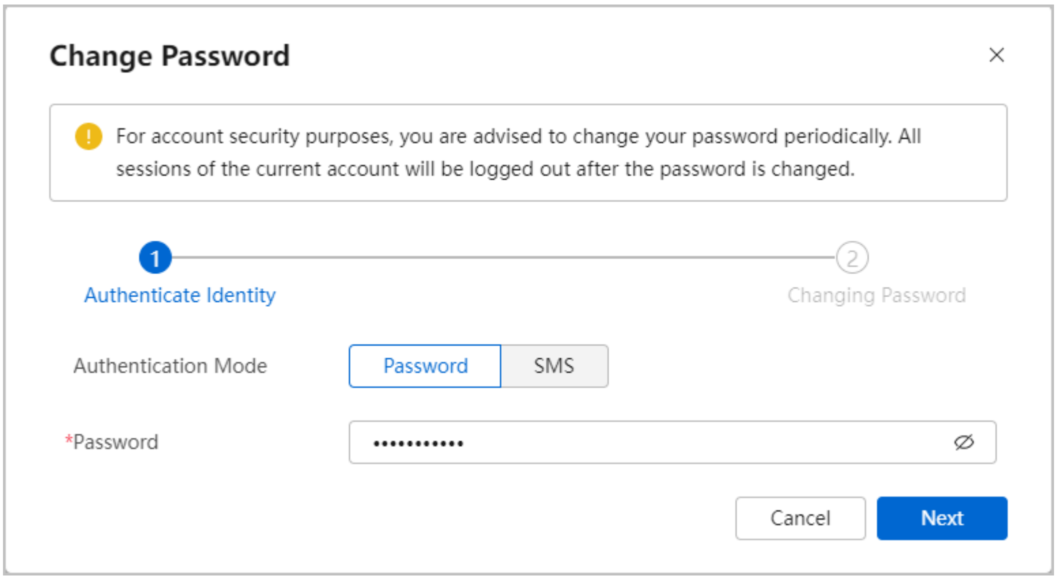
*Password: •••••••••••

NOTE

To change the linked phone number or email address, click ✎. The operations are similar to those in the linking process.

5. Change your password.
   a. Click ✎ on the right of the password.
   b. In the **Change Password** dialog box, enter your password or a verification code for identity verification, and click **Next**.

Figure 7-7 Verifying the identity



Change Password

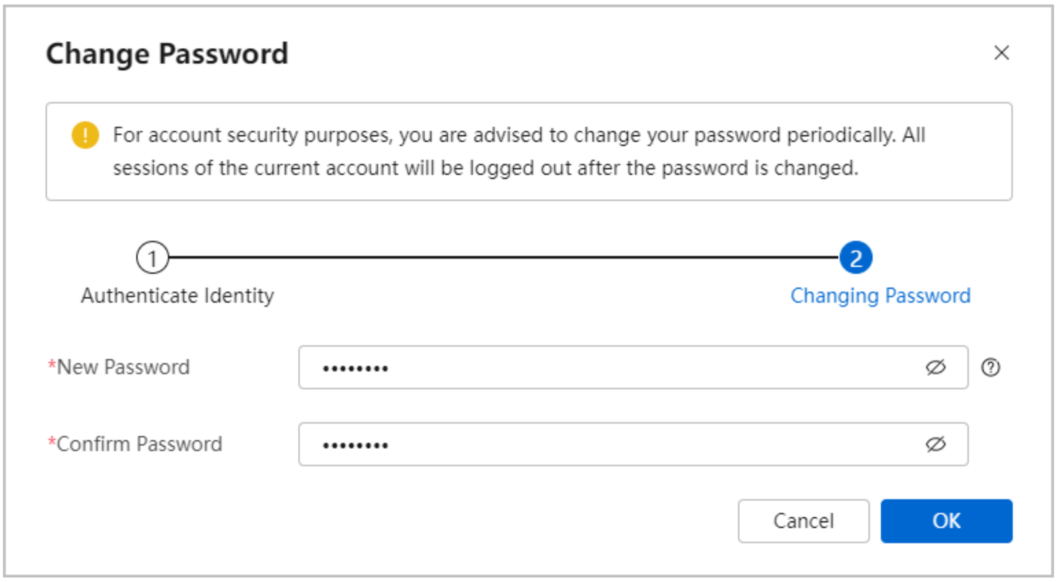
For account security purposes, you are advised to change your password periodically. All sessions of the current account will be logged out after the password is changed.

Authentication Mode: Password | SMS

*Password: ••••••••••••

   c. After successful verification, configure a new password, and click **OK**.

Figure 7-8 Changing the password



Change Password

For account security purposes, you are advised to change your password periodically. All sessions of the current account will be logged out after the password is changed.

*New Password: ••••••••

*Confirm Password: ••••••••

NOTE

If an email address has been linked, an email will be sent to this email address to notify the tenant of the password change success and the next password change time after the password is changed.

6. Enable dual-factor authentication. After this function is enabled, you need to enter both your password and an SMS verification code for identity authentication, further securing your account.

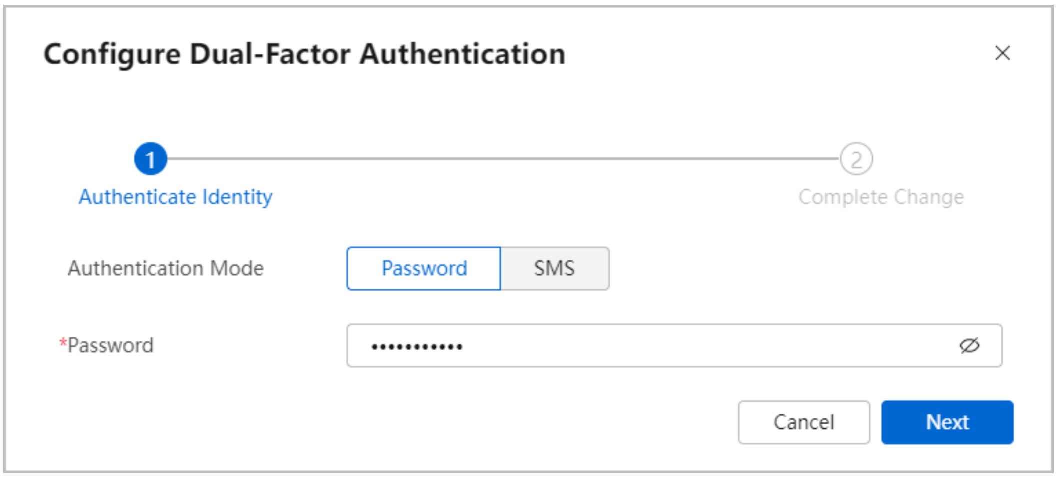
   NOTE

   Dual-factor authentication can be enabled only when you have set a password and linked a phone number to your account.

   a. Click 🔒 on the right of **Dual-Factor Auth**.

   b. Set **Authentication Mode** to **Password** or **SMS**, enter your password or a verification code for identity verification, and click **Next**.

   Figure 7-9 Verifying the identity



Configure Dual-Factor Authentication

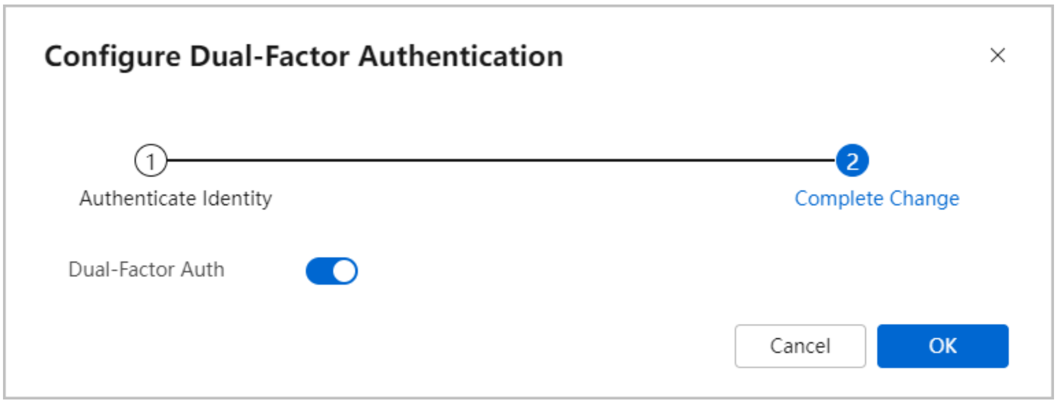
1 Authenticate Identity — 2 Complete Change

Authentication Mode: Password | SMS

*Password: ••••••••••••

   c. After successful verification, toggle on **Dual-Factor Auth** and click **OK**.

   Figure 7-10 Configuring dual-factor authentication



Configure Dual-Factor Authentication

1 Authenticate Identity — 2 Complete Change

Dual-Factor Auth: ●

7. Click **Export** in the upper right corner of **Personal Information** to export personal information.

NOTE

The exported Excel file contains personal data, such as the username, phone number, and email address. Therefore, keep the file safe.

MSP Information Settings

1. Log in to the console, click your account in the upper right corner, and click **Personal Center**.
2. In the **MSP Information** area, click **Upload** next to **Enterprise Logo**, and select a local image with a size no more than 10 MB.
3. Modify basic MSP information. Click ✎ on the right of a parameter such as the MSP name, industry, address, or phone number, and modify it as prompted.
4. Delete the MSP account.

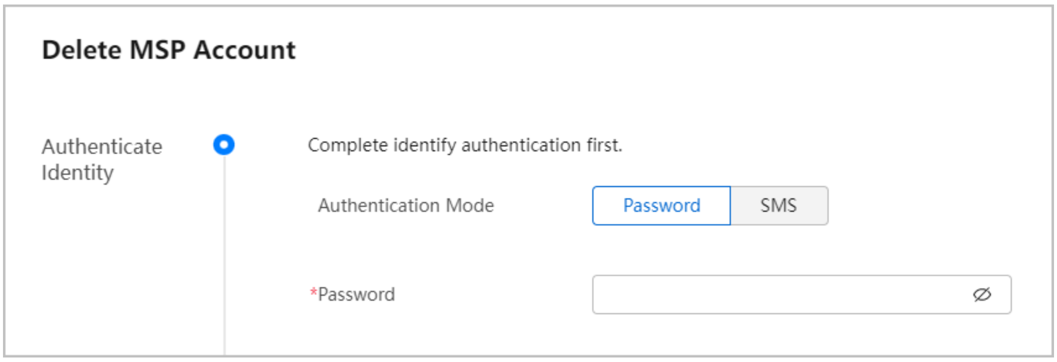
> ⚠ CAUTION
>
> - When your account is deleted, your data and services stored on the console will also be deleted and cannot be restored. Exercise caution when performing this operation.
> - Before deleting your account, ensure that the account does not have unfulfilled contracts, unsettled fees, unpaid taxes, or other obligations to be fulfilled according to applicable laws and regulations.

a. Click **Delete MSP Account** in the upper right corner, read the displayed information, and click **Delete MSP Account**.

b. Read through the account deletion precautions, select **I have read and agree to the Terms and Conditions on Deletion of Huawei Qiankun Accounts**, and click **Next**.

c. Enter your password or a verification code sent to your linked phone number for identity verification, and click **OK**.

Figure 7-11 Verifying the identity



Delete MSP Account

Authenticate Identity

Complete identify authentication first.

Authentication Mode: Password | SMS

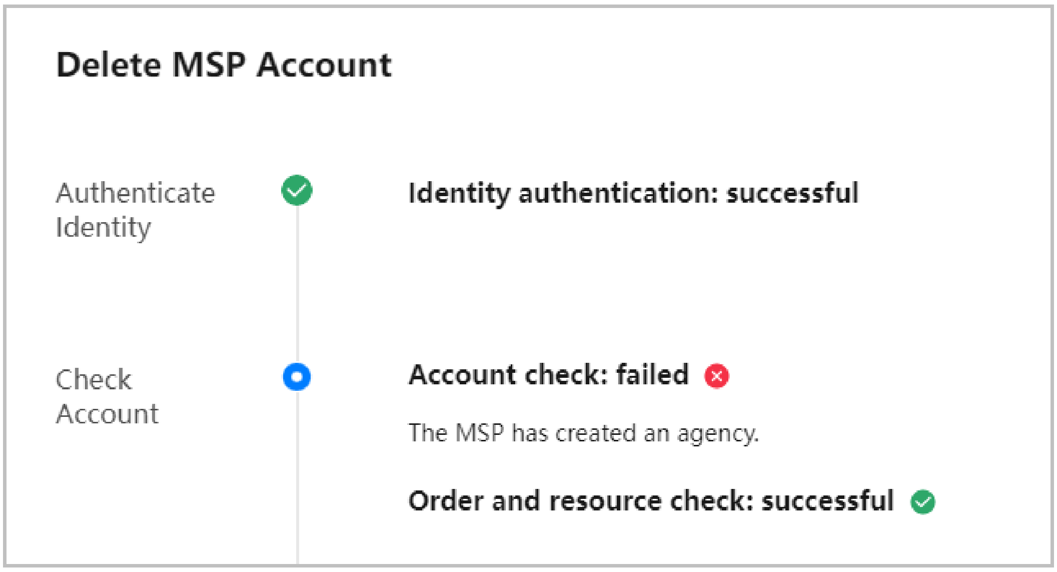
*Password

d. After successful account check, click **Delete MSP**.

- ▪ Account check: The system checks whether the current account has an agency relationship with an MSP. If so, delete the agency relationship before deleting the account.

- Oder and resource check: The system checks whether any services or resources are still in use under the current account. If so, release the services and resources before account deletion.

Figure 7-12 Checking the account



Delete MSP Account

Authenticate Identity ✓ Identity authentication: successful

Check Account ● Account check: failed ✕

The MSP has created an agency.

Order and resource check: successful ✓

e. Wait for a while. The current account is automatically logged out.

Viewing Website Agreements

1. Log in to the console, click your account in the upper right corner, and click **Personal Center**.
2. In the **Website Agreements** area, click **Privacy Statement** to view details.
3. Click **Huawei Qiankun Customer Agreement** to view details.
4. Click **Historical Signing** to view historical signing records, including the agreement version and signing scenario.

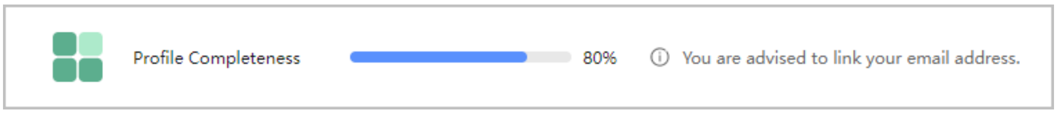
NOTE

If a website agreement is updated, you need to sign it upon login.

Profile Completeness

Click your account in the upper right corner of the console and click **Personal Center** to view the profile completeness of your current account. You can link a phone number or email address to your account as prompted.

Figure 7-13 Profile completeness



Profile Completeness 80% ⓘ You are advised to link your email address.

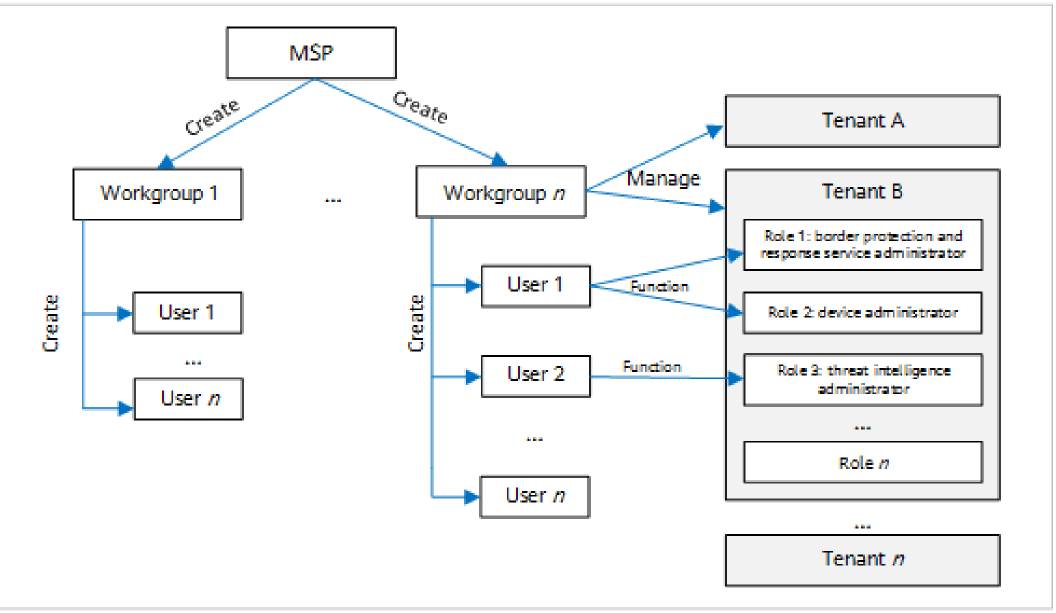
8 MSP Account Management

8.1 Context

For details about the MSP accounts of Huawei Qiankun, see **3 MSP Account Types**. The rights- and domain-based management principle of MSP accounts is similar to that of tenant accounts. MSP accounts can be managed in MSP workgroups at multiple levels.

As shown in **Figure 8-1**, MSP workgroups are organized in an enterprise-like hierarchy. They can be divided based on the organization structure, and MSP users in each workgroup are assigned with specified permissions. This implements rights- and domain-based management.

Figure 8-1 Rights- and domain-based MSP design



Workgroup

Domain-based management is implemented on a per-workgroup basis.

The system provides a default workgroup, which is also called a root workgroup. The first registered MSP account is the root workgroup administrator, acting the role of a tenant administrator with all operation permissions. To ensure system security, the **admin** user can create multiple sub-accounts and assign different permissions to each sub-account based on the account role.

The sub-accounts and user roles created by an administrator are not isolated. As such, horizontal privilege escalation may occur, which brings security risks. For example, the default root administrator account, who has the highest permissions, creates accounts A and B, and assigns the accounts to subordinate departments or partners, respectively. If both accounts A and B have the account management and role management permissions, they can modify and delete accounts and roles of each other.

To prevent horizontal privilege escalation, you can configure workgroups to isolate accounts and user roles created by administrators. Workgroups are configured a hierarchical tree structure, that is, upper-level workgroups grant permissions to lower-level workgroups. Users in a workgroup can maintain accounts and user roles in their own workgroup and lower-level workgroups. Different accounts in parallel work groups have different authority, with data invisible to each other. To prevent horizontal privilege escalation, the default root administrator can assign workgroup administrator accounts, instead of sub-accounts, to subordinate departments or branches.

NOTE

The administrator of the root workgroup can create lower-level workgroups based on the following rules:

- Each workgroup has an administrator. By default, the administrator of a workgroup can create users in the same workgroup. Common users (not the administrator) in a workgroup can create users in the workgroup only after being authorized.
- A maximum of five levels of workgroups are supported. By default, a workgroup is created, modified, or deleted by the administrator of the upper-level workgroup. Common users in the upper-level workgroup can create, modify, or delete lower-level workgroups only after being authorized.

User

A user refers to a person who uses the system. Information about a user includes a username, password, and permissions.

Users can be divided into the following types:

- Local: refers to a common user.
- Third-party: refers to a user who logs in to the console by invoking a northbound API. They are also known as northbound users.
- Remote: refers to a Huawei website user who needs to click **Huawei Website Account** when logging in to the Huawei Qiankun console.

Role

A role is a collection of user operation permissions. The operation permissions of an MSP depend on the roles assigned when the MSP or workgroup is created.

The Huawei Qiankun console supports two types of MSP roles: public roles and service roles.

To facilitate MSP operations, custom roles can be configured on the console. For details, see **Table 8-1**.

Table 8-1 MSP roles supported by Huawei Qiankun

Role Type	Role Name	Description
Public role	MSP administrator	Has the read and write permissions for all MSP services and related configurations.
	MSP auditor	Has the read permissions for all MSP services and related configurations.
	MSP open API operator	Has permissions for open API services and related configurations.
Service role **NOTE** For more information, see related sections about the MSP permission control of each service.	Common service role	Has read and write permissions for some common services, such as the service ticket service, topic subscription service, and audit log service. **NOTE** Ordinary MSP accounts (not MSP administrators or auditors) have operation permissions on specific services, such as service ticket management, subscription management, and log viewing, only after they are assigned the corresponding service roles.
Custom role	Custom role	You can assign operation permissions to such a role based on your site requirements.

8.2 Creating a Role

Prerequisites

You have logged in to the Huawei Qiankun console and have one of the permissions of the following roles:

- Preset role: MSP administrator permission

- Custom role: role management permission of the user and tenant service

Context

The operation permissions of an MSP for using Huawei Qiankun are determined by the roles assigned to the MSP.

The console provides preset roles for each service. MSPs can also configure custom roles.

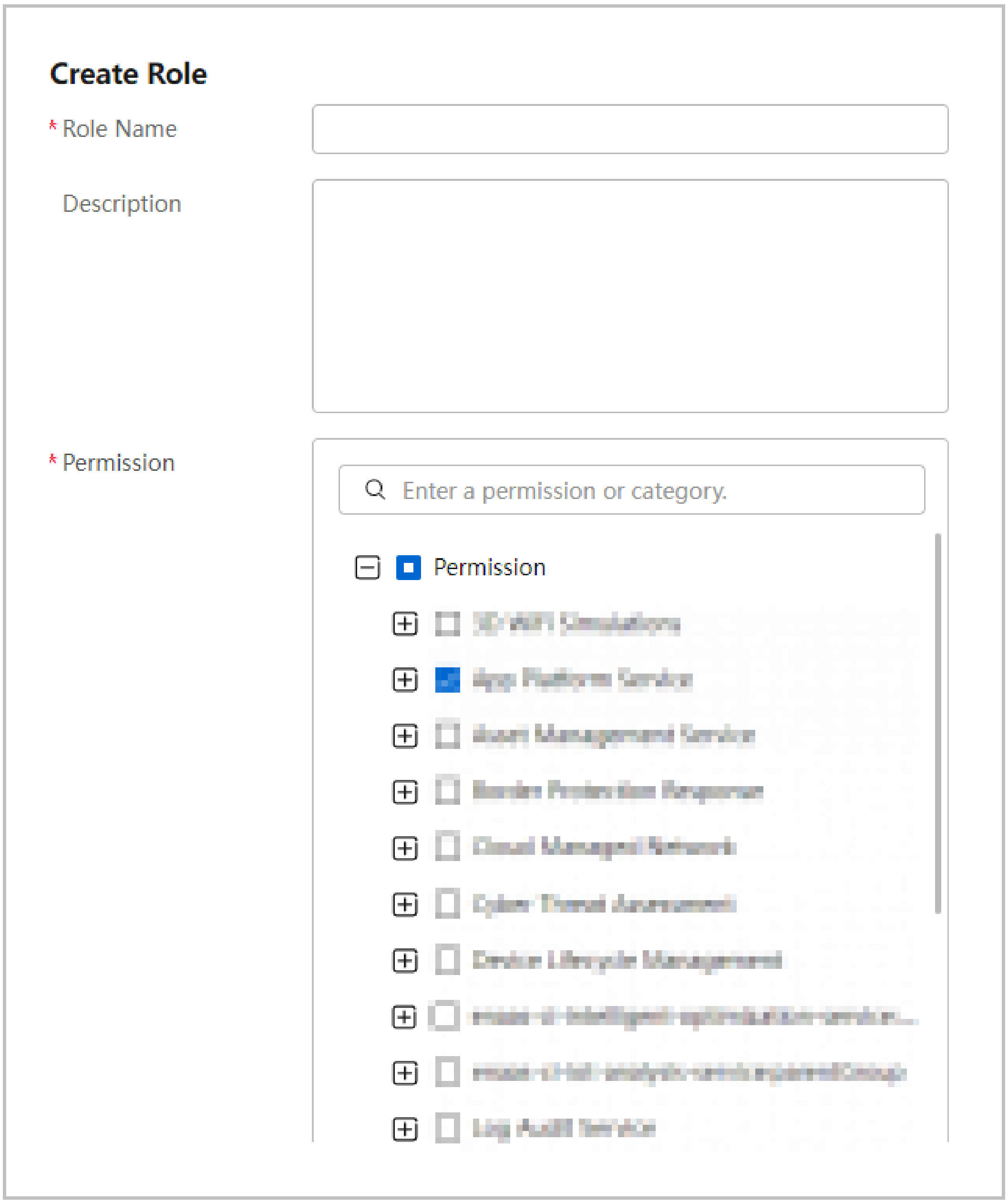
Procedure

Step 1 Click your account in the upper right corner, and choose **Permission Management** > **Role Management**. The **Role Management** page is displayed.

Step 2 Click **Create**, enter the name of a custom role, specify operation permissions, and click **OK**.

Upon creation, a role can be assigned to MSP users in lower-level workgroups.

Figure 8-2 Creating a role



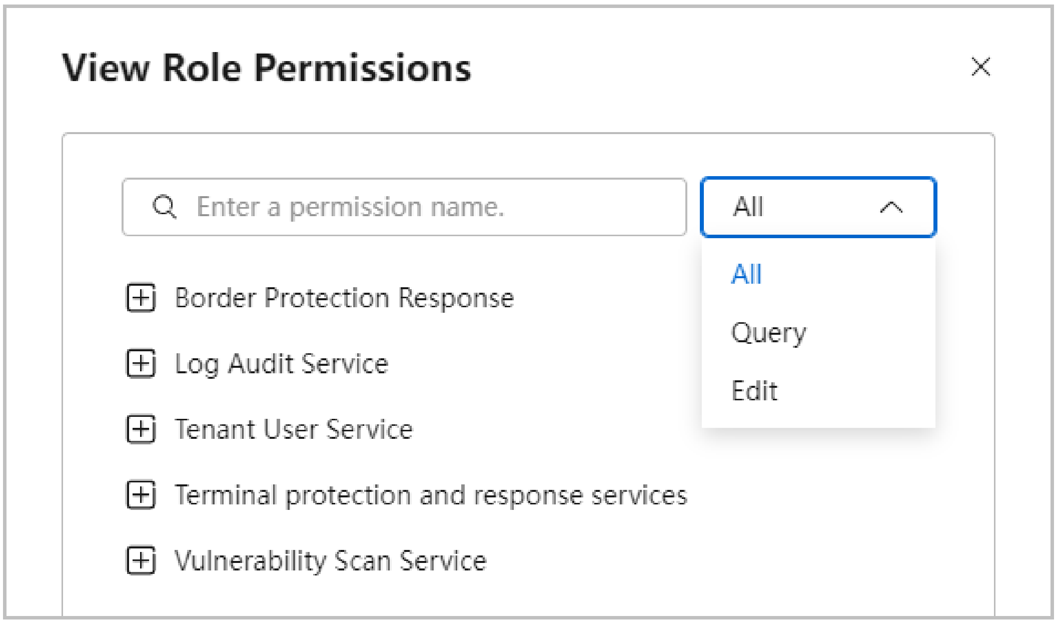
----End

Follow-up Procedure

Custom roles support the view, modify, delete, and search operations on permissions, whereas preset roles support only the view and search operations on permissions.

- View: Select a role and click 🔍 in the **Operation** column to view its permissions. In the **View Role Permissions** dialog box, you can further filter the query or edit permissions of the role.

Figure 8-3 Viewing permissions of a role



View Role Permissions ×

Enter a permission name.

All
- All
- Query
- Edit

- ⊞ Border Protection Response
- ⊞ Log Audit Service
- ⊞ Tenant User Service
- ⊞ Terminal protection and response services
- ⊞ Vulnerability Scan Service

- Search: Enter a role name in the search box, and click 🔍 on the left or press **Enter** to search for the role.
- Modify: Select a role, and click ✎ in the **Operation** column to modify the operation permissions of the role.
- Delete: Select a role, and click 🗑 in the **Operation** column or **Delete** above the user list to delete the role. If a role has been assigned to a lower-level workgroup, operation permissions of this workgroup will be affected after the role is detected. Therefore, exercise caution when deleting a role.

8.3 Creating a Workgroup

Prerequisites

You have logged in to the Huawei Qiankun console and have one of the permissions of the following roles:

- Preset role: MSP administrator permission
- Custom role: permission to manage workgroups and managed objects under the user and tenant service

Context

The first registered MSP account is the root workgroup administrator, acting the role of a tenant administrator with all operation permissions.

The root workgroup administrator can create lower-level workgroups. A maximum of five levels of workgroups are supported, and each workgroup has an administrator.

Procedure

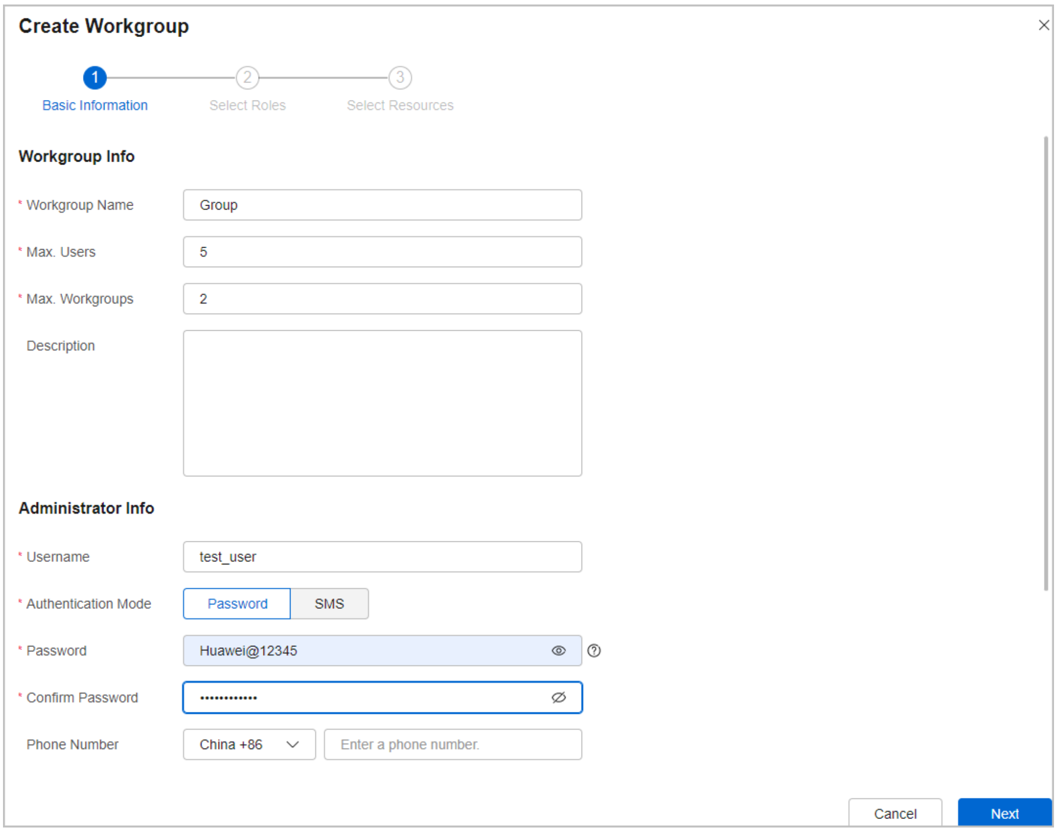
Step 1 Click your account in the upper right corner, and choose **Permission Management** > **User Management**. The **User Management** page is displayed.

Step 2 In the workgroup navigation tree, click **+** to create a workgroup.

Step 3 Configure basic workgroup information and administrator information, and click **Next**. For details about the parameters, see **Table 8-2**.

- The value of **Max. Users** or **Max. Workgroups** cannot exceed the number of remaining users or workgroups supported by the root workgroup.
- To view information about the root workgroup, click next to **Default Workgroup**.

Figure 8-4 Configuring workgroup information



Create Workgroup

Workgroup Info

* Workgroup Name: Group

* Max. Users: 5

* Max. Workgroups: 2

Description:

Administrator Info

* Username: test_user

* Authentication Mode: Password

* Password: Huawei@12345

* Confirm Password: ••••••••••••

Phone Number: China +86 | Enter a phone number.

Table 8-2 Parameters for configuring a workgroup administrator

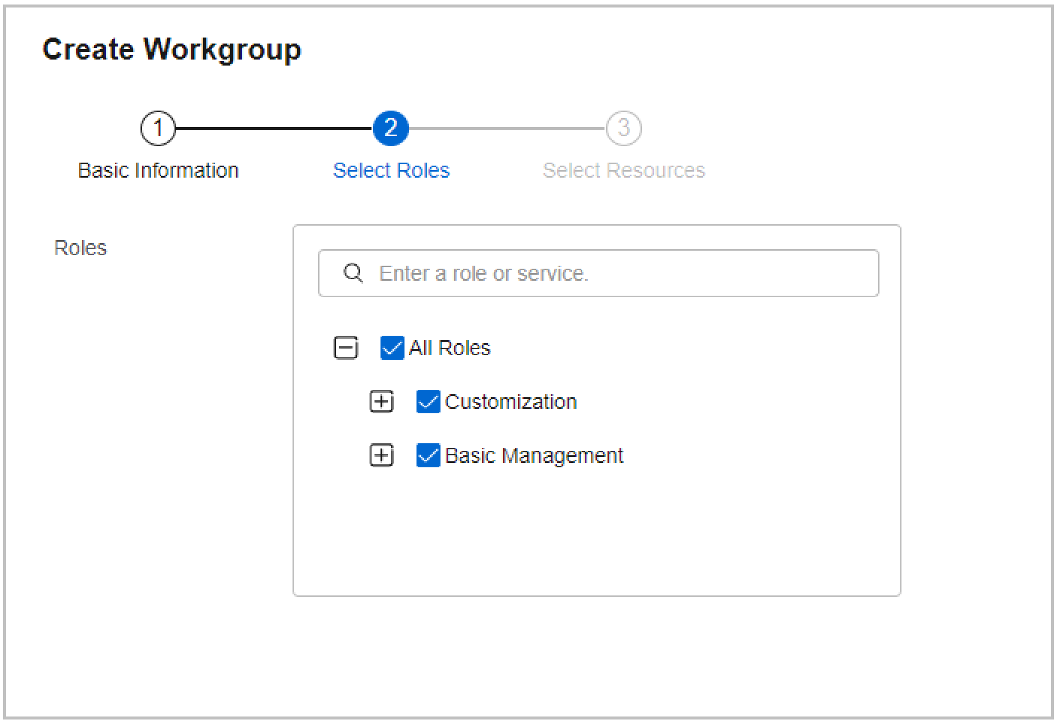
Parameter	Description
Authentication Mode	Administrator authentication mode, which can be set to **Password** or **SMS**.
Password	Password of the administrator. Set a password that complies with **password requirements**.

Parameter	Description
Phone Number, Email Address	Phone number or email address for receiving notifications and reports from Huawei Qiankun.
Enable User	Whether to enable the workgroup administrator. The workgroup administrator is enabled by default, indicating that this user is online and can perform operations allowed by its authorized permissions.

Step 4 Specify roles for the workgroup administrator, and click **Next**.

- By default, the role list displays all roles of the current login account.
- In this example, the default roles of a tenant are displayed. If you have created a custom role by referring to **8.2 Creating a Role**, the role is also displayed in the role list.

Figure 8-5 Specifying administrator roles



Create Workgroup

Roles

Enter a role or service.

⊟ ☑ All Roles

⊞ ☑ Customization

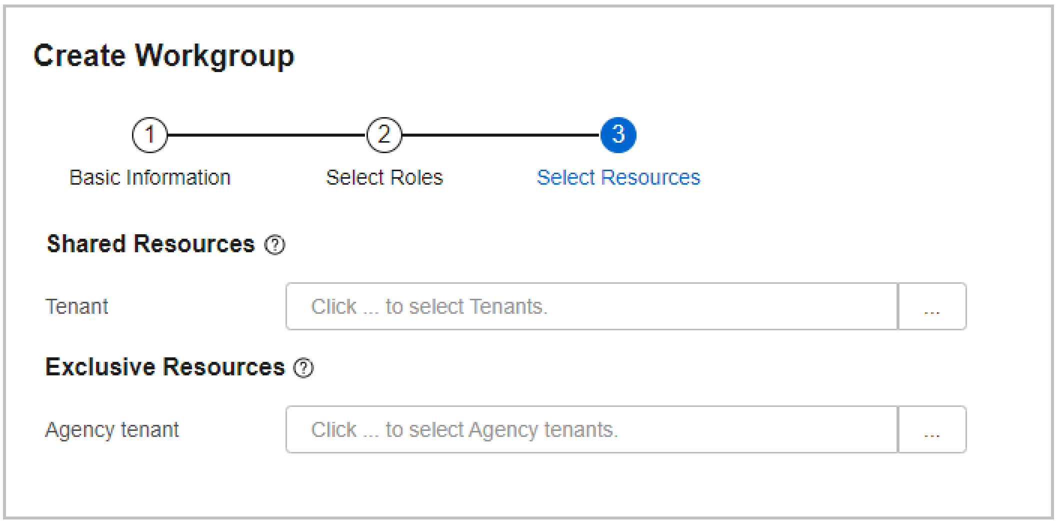
⊞ ☑ Basic Management

Step 5 Configure managed resources for the workgroup, and click **Finish**.

- **Shared Resources**: refers to self-created tenants, which can be managed by multiple workgroups at the same level.
- **Exclusive Resources**: refer to managed tenants, which can be managed by only one workgroup at the same level.

Managed tenants or self-created tenants can be managed by users in a workgroup only after being allocated to the workgroup.

Figure 8-6 Configuring a managed object



Create Workgroup

Shared Resources

Tenant: Click ... to select Tenants. ...

Exclusive Resources

Agency tenant: Click ... to select Agency tenants. ...

----End

Follow-up Procedure

- Change the initial password. When logging in to the Huawei Qiankun console for the first time, the new workgroup administrator needs to sign website agreements and change the password.
- View, modify, or delete a workgroup. The root workgroup can only be viewed.

Table 8-3 Operations that can be performed on workgroups

Operation	Description
View	Select a workgroup in the **Workgroups** navigation tree, and click 🔍 above the user list to view the workgroup information, administrator information, and managed objects.
Modify	Select a workgroup in the **Workgroups** navigation tree, and click ✎ above the user list to modify the workgroup information, such as the workgroup name, maximum number of users, and managed objects.

Operation	Description
Delete	● Deleting a single user: Select a user and click 🗑 in the **Operation** column. ● Deleting users in batches: Select multiple users and click **Delete** above the user list to delete the users. **CAUTION** ● To delete a workgroup with lower-level groups, delete its lower-level workgroups first. A workgroup with lower-level workgroups cannot be deleted. ● When a workgroup is deleted, all data and user information of the workgroup will also be deleted and cannot be restored, and online users in the workgroup will be logged out. Exercise caution when performing this operation.

8.4 Creating a User

Prerequisites

You have logged in to the Huawei Qiankun console and have one of the permissions of the following roles:

- Preset role: tenant administrator permission
- Custom role: user management permission of the user and tenant service

Context

By default, only the administrator of a workgroup can create users.

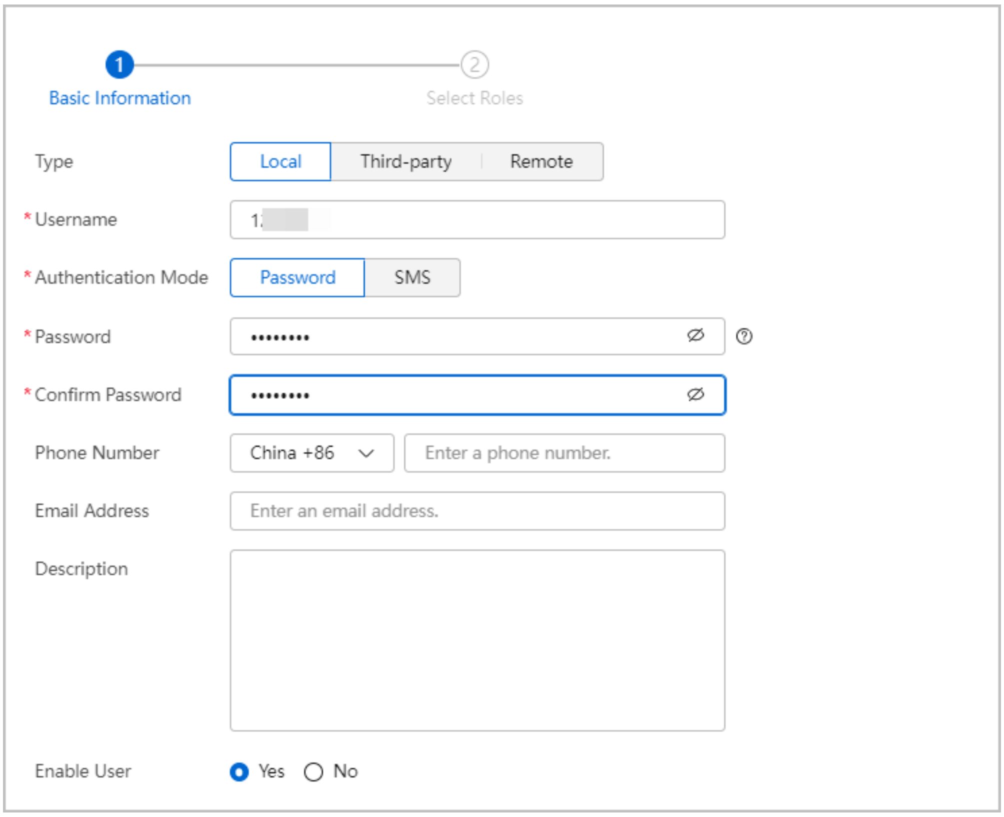
A common user can create users only after being assigned the user management permission.

Procedure

Step 1 Click your account in the upper right corner, and choose **Permission Management** > **User Management**. The **User Management** page is displayed.

Step 2 Click **Create** above the user list, configure user information based on **Table 8-4**, and click **Next**.

Figure 8-7 Configuring basic user information



1 Basic Information
2 Select Roles

Type: Local | Third-party | Remote

* Username: 1[redacted]

* Authentication Mode: Password | SMS

* Password: ••••••••

* Confirm Password: ••••••••

Phone Number: China +86 | Enter a phone number.

Email Address: Enter an email address.

Description:

Enable User: ● Yes ○ No

Table 8-4 Parameters for configuring a user

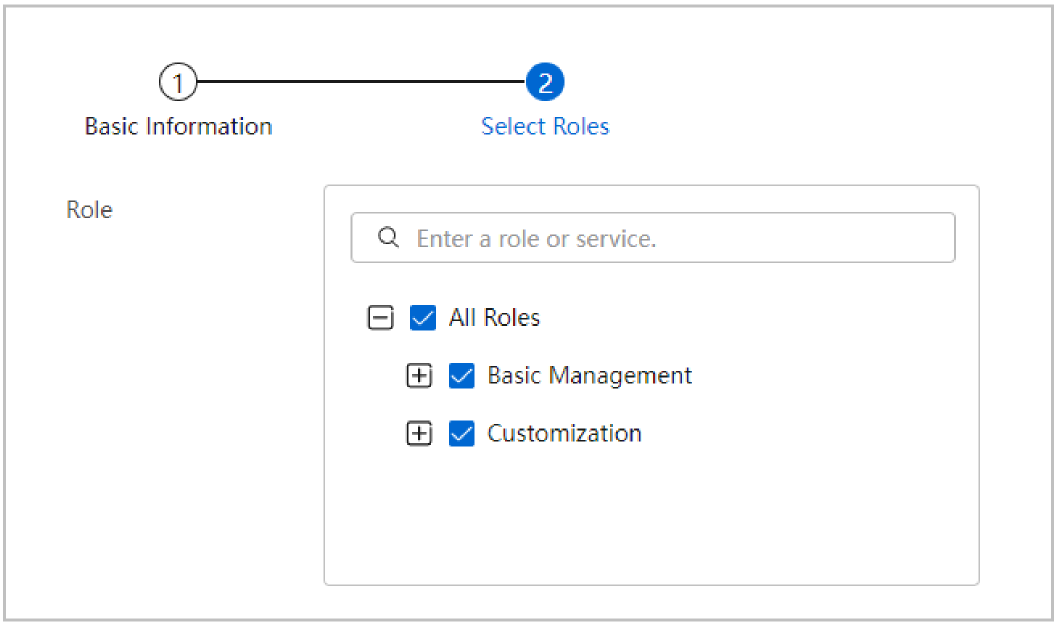
Parameter	Description
Type	● **Local**: refers to a common user. ● **Third-party**: refers to a user who logs in to the console by invoking a northbound API. They are also known as northbound users. ● **Remote**: refers to a Huawei website user. **NOTE** Only users who have the user management permission of the user and tenant service in the root workgroup can create third-party system users.
Authentication Mode	Administrator authentication mode, which can be set to **Password** or **SMS**.
Password	Password of the user.
Phone Number, Email Address	Phone number or email address for receiving notifications and reports from Huawei Qiankun.
Enable User	This function is enabled by default. If this function is disabled, the user account cannot be used to log in to the console and the assigned permissions do not take effect.

Parameter	Description
Password Change at Initial Login	Forcibly asks a user to change the password at the initial login. This parameter is available only when **Type** is set to **Third-party**. This function is enabled by default. If this function is disabled, password change is optional upon the initial login.

Step 3 Select roles based on the site requirements, and click **Finish**.

- By default, the role list displays all roles of the current login account.
- To assign other roles, create them in advance by referring to **8.2 Creating a Role**.

Figure 8-8 Selecting user roles



----End

Follow-up Procedure

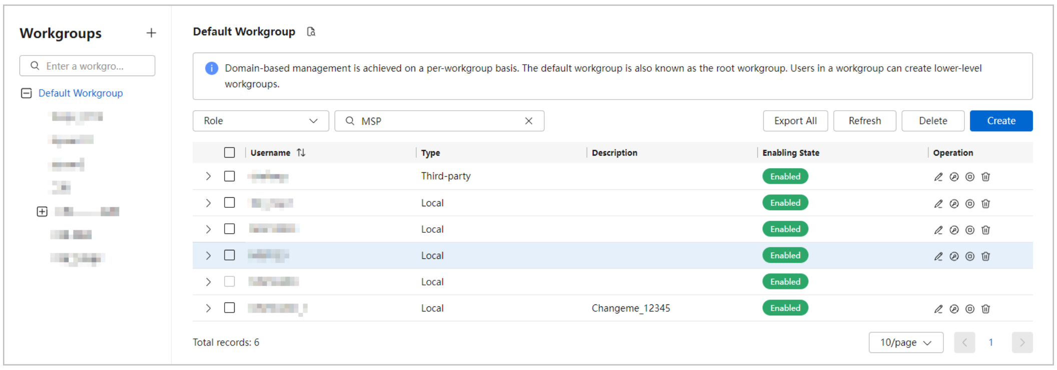
- Change the initial password. When logging in to the Huawei Qiankun console for the first time, the new user needs to sign website agreements and change the password.
- Edit user information. Workgroup users can be modified, disabled, deleted, and exported, and their passwords can be reset. **Table 8-5** describes these operations in detail.

Table 8-5 Operations that can be performed on a workgroup user

Operation	Description
Modify	Select a user and click ✎ in the **Operation** column to modify the phone number, email address, and roles.
Password reset	Select a user and click ⊙ in the **Operation** column to reset the user password. Once the password is reset, the system logs out all current sessions of the user.
Enable/ Disable	- Select a user and click ◎ in the **Operation** column to disable the user. If the user is online, the user is logged out. - Select a disabled user and click ▷ in the **Operation** column to enable the user.
Delete	- Deleting a single user: Select a user and click 🗑 in the **Operation** column. - Deleting users in batches: Select multiple users and click **Delete** above the user list. **CAUTION** Exercise caution when performing this operation because a user cannot be restored after being deleted.
Export	Select a workgroup in the **Workgroups** navigation tree, and click **Export All** above the user list. **NOTE** The exported Excel file contains personal data, such as usernames, user types, enabling states, phone numbers, and email addresses. Therefore, keep the file safe.

- Search for users.
  a. On the **User Management** page, select a workgroup in the **Workgroups** navigation tree.
  b. Select **Username/Description** or **Role** from the drop-down list box.
  c. Enter a keyword in the search box and press **Enter**.

Figure 8-9 Searching for users by role



Domain-based management is achieved on a per-workgroup basis. The default workgroup is also known as the root workgroup. Users in a workgroup can create lower-level workgroups.

□ Username	Type	Description	Enabling State	Operation
□ [redacted]	Third-party		Enabled	
□ [redacted]	Local		Enabled	
□ [redacted]	Local		Enabled	
□ [redacted]	Local		Enabled	
□ [redacted]	Local		Enabled	
□ [redacted]	Local	Changeme_12345	Enabled	

Total records: 6

9 Tenant Agency Processment

Prerequisites

You have logged in to the Huawei Qiankun console as a top-level MSP workgroup user and have the tenant management permission of an MSP administrator.

Context

- When receiving an agency application or an agency change application from a tenant, an MSP can either approve or reject the application. An agency relationship between the tenant and the MSP is established or changed only after application approval.
- An MSP can also initiate an agency termination application to a tenant. The agency relationship between the MSP and the tenant is terminated only after application approval.

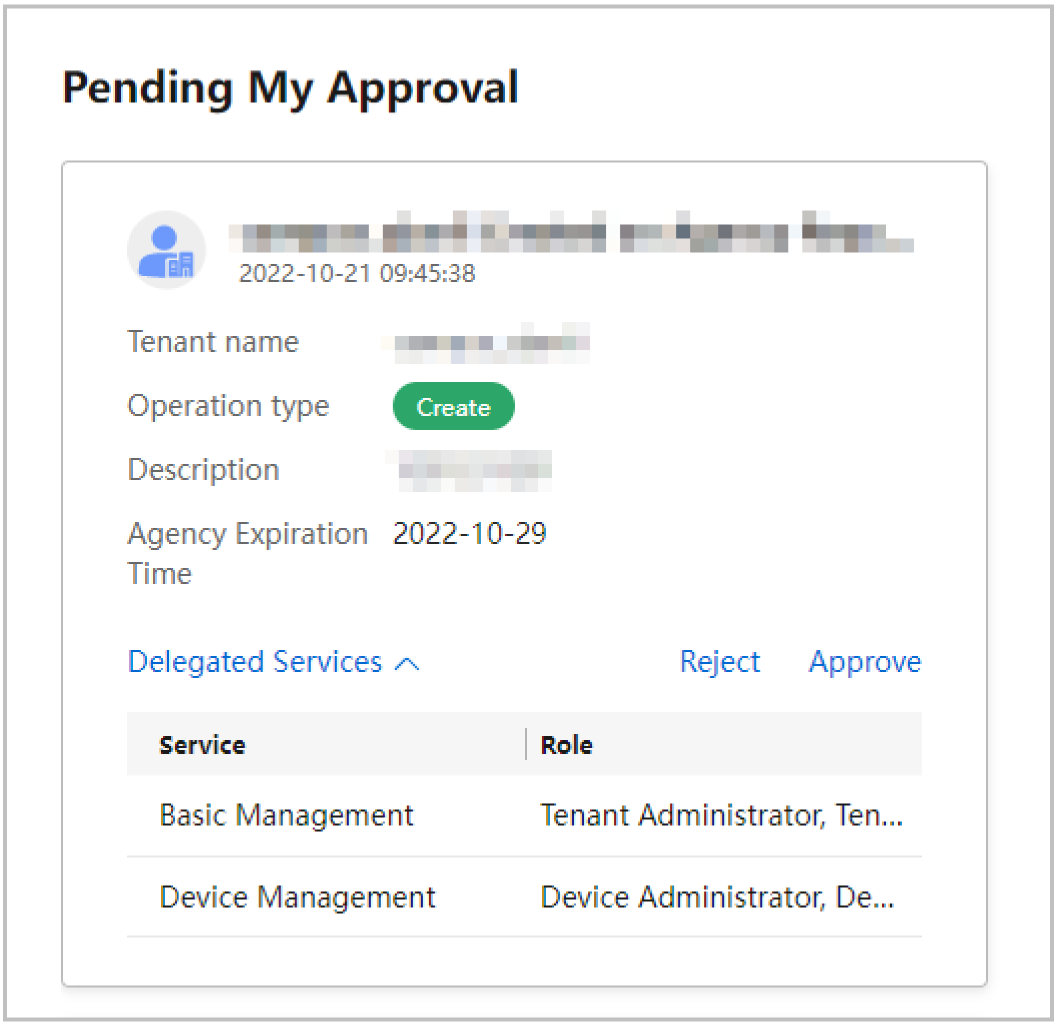
Procedure

1. Click your account in the upper right corner of the console, and choose **Agencies**.
2. Handle an agency application.

   View agency service applications and related descriptions provided by tenants on the **Pending My Approval** page. You can either click **Reject** or **Approve**.

   - **Approve**: If you select **Approve**, enter an approval comment, select the "**I understand and agree that as a delegated party, I shall exercise rights only within the scope of authorization and shall bear corresponding legal consequences for any behavior beyond the scope of authorization**" check box, and click **OK**.
   - **Reject**: If you select **Reject**, enter a rejection comment and click **OK**.

Figure 9-1 Pending My Approval page



Pending My Approval

[redacted]
2022-10-21 09:45:38

Tenant name [redacted]

Operation type Create

Description [redacted]

Agency Expiration Time 2022-10-29

Service	Role
Basic Management	Tenant Administrator, Ten...
Device Management	Device Administrator, De...

3. Delete an agency.

⚠ CAUTION

After the agency relationship between the entrusting and entrusted parties is deleted, the data of the entrusting party cannot be maintained. Ensure that the entrusting party is aware of the deletion, with a consensus reached by the two parties.

To initiate an agency deletion application, click 🗑 on an agency relationship and wait for the tenant's approval.

4. View agencies.

On the **Agency** page, click **Agency Records** to view the initiated and approved applications. You can click ↩ to cancel an application in the **Pending approval** state.

10 Tenant Management

Prerequisites

You have logged in to the Huawei Qiankun console and have the tenant management permission of the user and tenant service.

Context

MSPs can manage tenant information on Huawei Qiankun. They can quickly create, search, modify, and export information about tenants.

NOTE

Both users in the top-level or lower-level MSP workgroups can create tenant accounts.

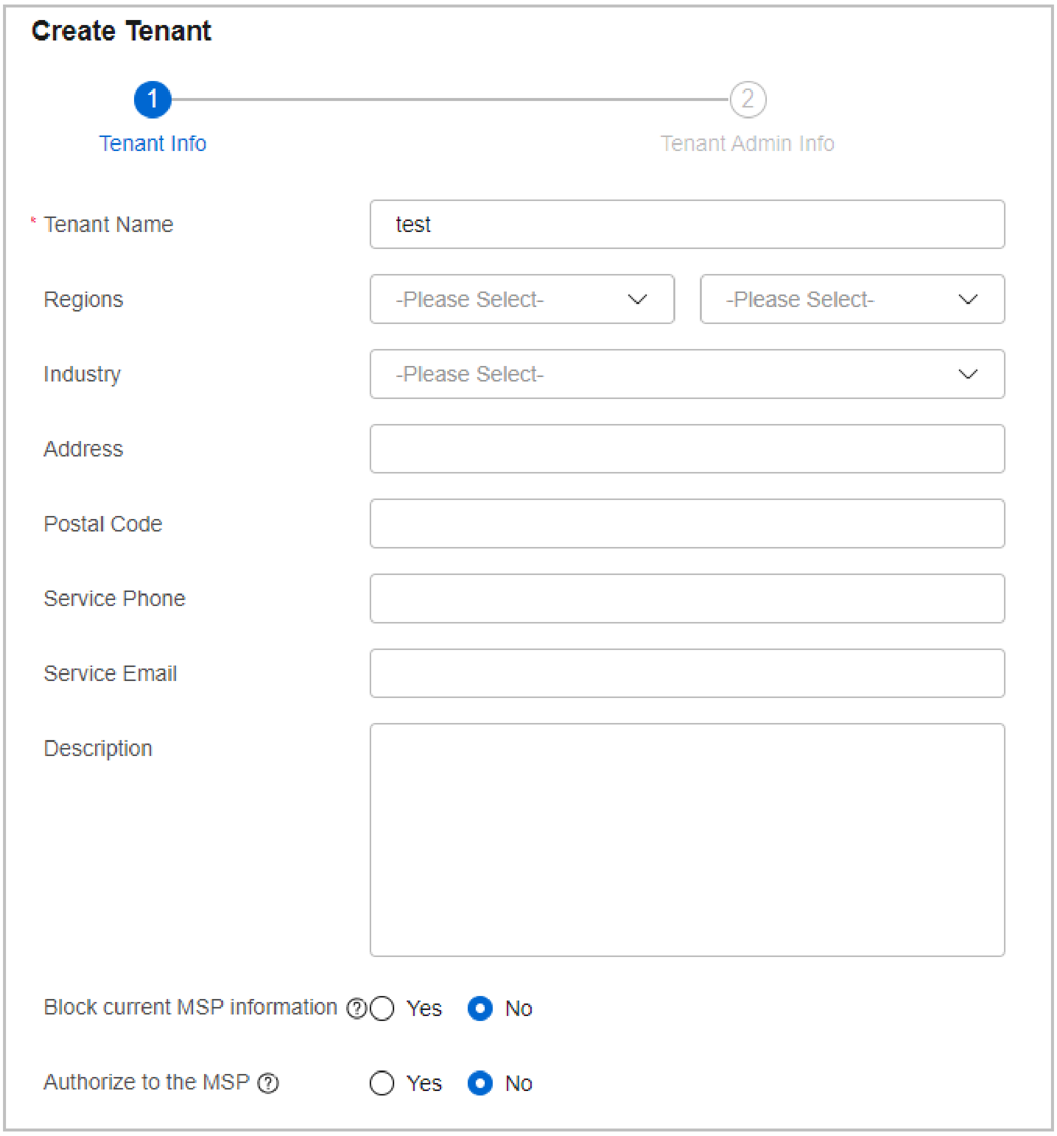
Procedure

Step 1 Click **Tenants** in the upper right corner of the console. The **Managed Tenants** page is displayed.

Step 2 Create a tenant account.

1. Select **Self-created Tenants** and click **Create** above the tenant list.
2. Enter the tenant information and click **Next**.

Figure 10-1 Configuring self-created tenant information



Create Tenant

1 Tenant Info

2 Tenant Admin Info

* Tenant Name: test

Regions: -Please Select- -Please Select-

Industry: -Please Select-

Address:

Postal Code:

Service Phone:

Service Email:

Description:

Block current MSP information ○ Yes ● No

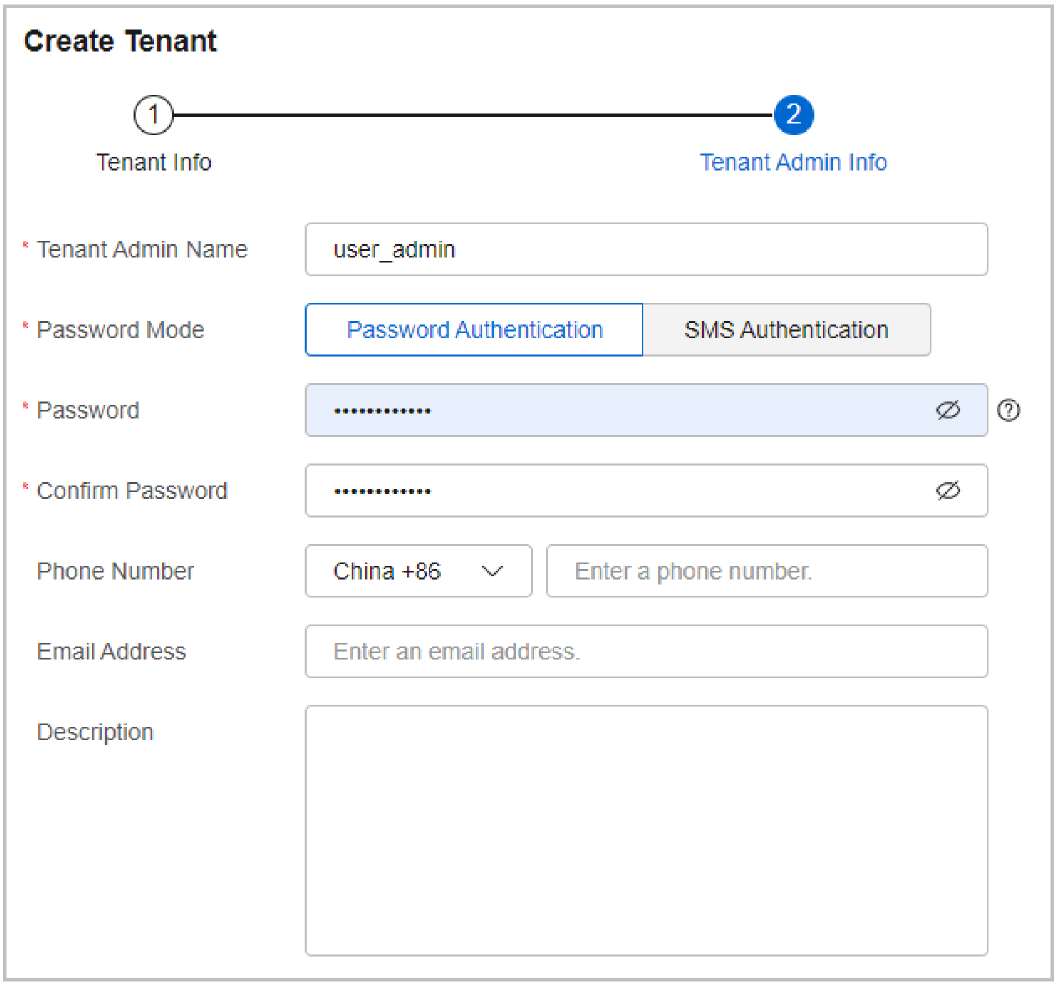
Authorize to the MSP ○ Yes ● No

NOTE

- During the tenant account creation, **Authorize to the MSP** is set to **No** by default. If **Authorize to the MSP** is set to **Yes**, you need to set **Agency Expiration Time** and accept the risk notification agreement.
- During the tenant account creation, **Block current MSP information** is set to **No** by default. If **Block current MSP information** is set to **Yes**, the current MSP information will not be detected.
- By default, the MSP automatically has the operation permissions on the public roles assigned to a new tenant. However, the service role assigned to the current tenant after a new service is purchased will not be automatically entrusted to the MSP.

3. Configure tenant administrator information, set a password that complies with **password requirements**, and click **Finish**.

Figure 10-2 Configuring self-created tenant administrator information



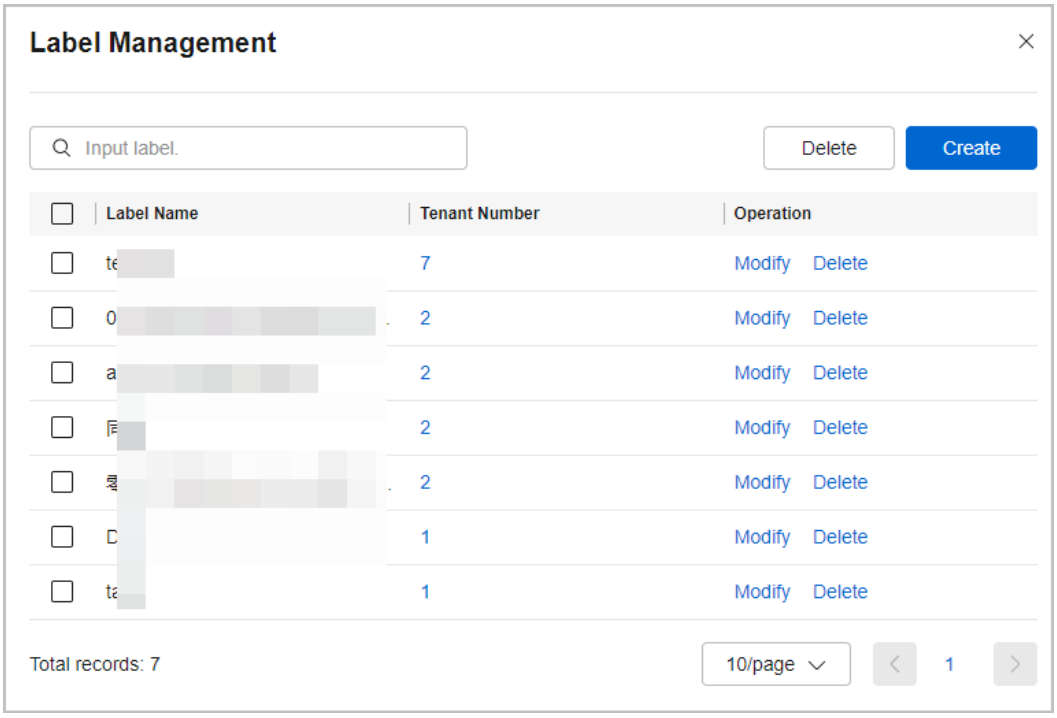
Create Tenant

* Tenant Admin Name	user_admin
* Password Mode	Password Authentication / SMS Authentication
* Password	••••••••••••
* Confirm Password	••••••••••••
Phone Number	China +86 / Enter a phone number.
Email Address	Enter an email address.
Description	

Step 3 (Optional) Create a tenant label.

1. On the **Managed Tenants** page, click 🏷 above the tenant list to access the **Label Management** page.

Figure 10-3 Managing labels



Label Management

Input label.

Delete | Create

☐	Label Name	Tenant Number	Operation
☐	te	7	Modify Delete
☐	0	2	Modify Delete
☐	a	2	Modify Delete
☐	同	2	Modify Delete
☐	零	2	Modify Delete
☐	D	1	Modify Delete
☐	ta	1	Modify Delete

Total records: 7

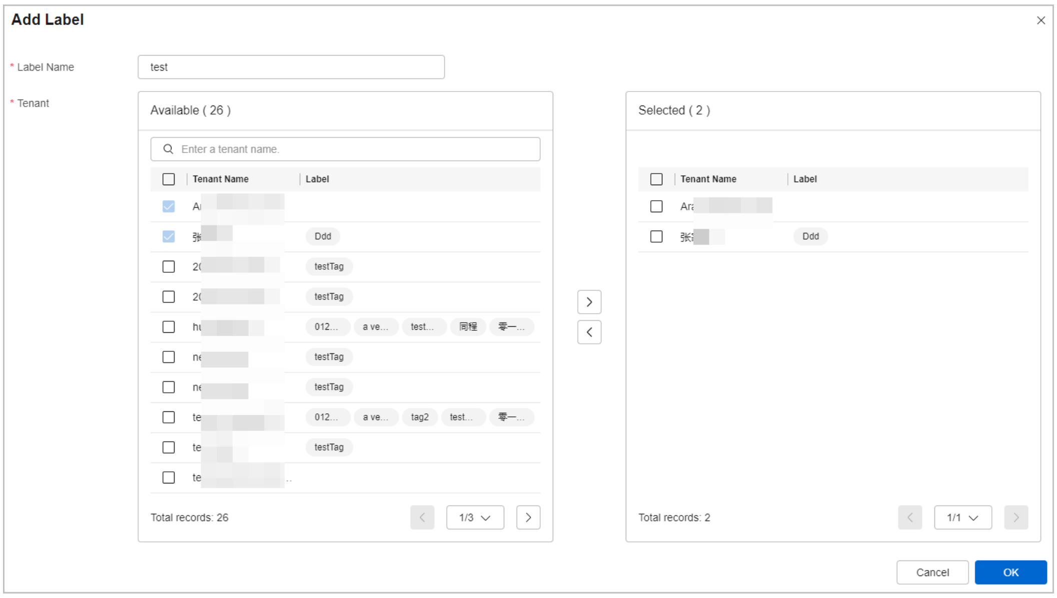
10/page 1

NOTE

You can click a number in the **Tenant Number** column of a label and add the label to multiple tenants.

2. On the **Label Management** page, click **Create** to create a label for tenants.

Figure 10-4 Creating a label



Add Label

* Label Name: test

* Tenant

Available (26)

Enter a tenant name.

☐	Tenant Name	Label
☑	A	
☑	张	Ddd
☐	2	testTag
☐	2	testTag
☐	h	012... a ve... test... 同程 零一...
☐	n	testTag
☐	n	testTag
☐	te	012... a ve... tag2 test... 零一...
☐	te	testTag
☐	te	..

Total records: 26 1/3

Selected (2)

☐	Tenant Name	Label
☐	Ar	
☐	张	Ddd

Total records: 2 1/1

Cancel | OK

3. On the **Add Label** page, enter a label name, select tenants, and click **OK**.

NOTE

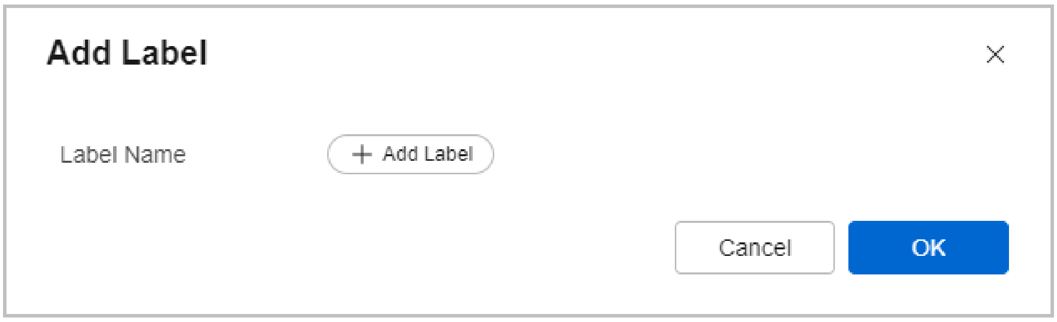
- You can click 🏷 after a username to add a label for it. The label is displayed under the tenant name in the list.
- A label can be added to a maximum of 100 tenants, and an MSP account can have a maximum of 100 labels.
- A maximum of five labels can be added to a tenant.

----End

Follow-up Procedure

- Search the tenant information by label. Select **Managed Tenants** and click ⊽ above the tenant list to search managed tenants by label.
- Add a tenant label. Click 🏷 after a tenant name to add a label to it. In the **Add Label** dialog box that is displayed, click **+Add Label** to add a label to the tenant. A maximum of five labels can be added to a tenant.

  Figure 10-5 Adding a label

- Delete a tenant label. If a label is no longer needed, click × next to the label name to remove the label.
- Search for tenant information. Select **Self-created Tenants** or **Managed Tenants**, enter key information above the tenant list, and click 🔍 or press **Enter**.
- Export tenant information. Select **Self-created Tenants** or **Managed Tenants** and click **Export All** above the tenant list.

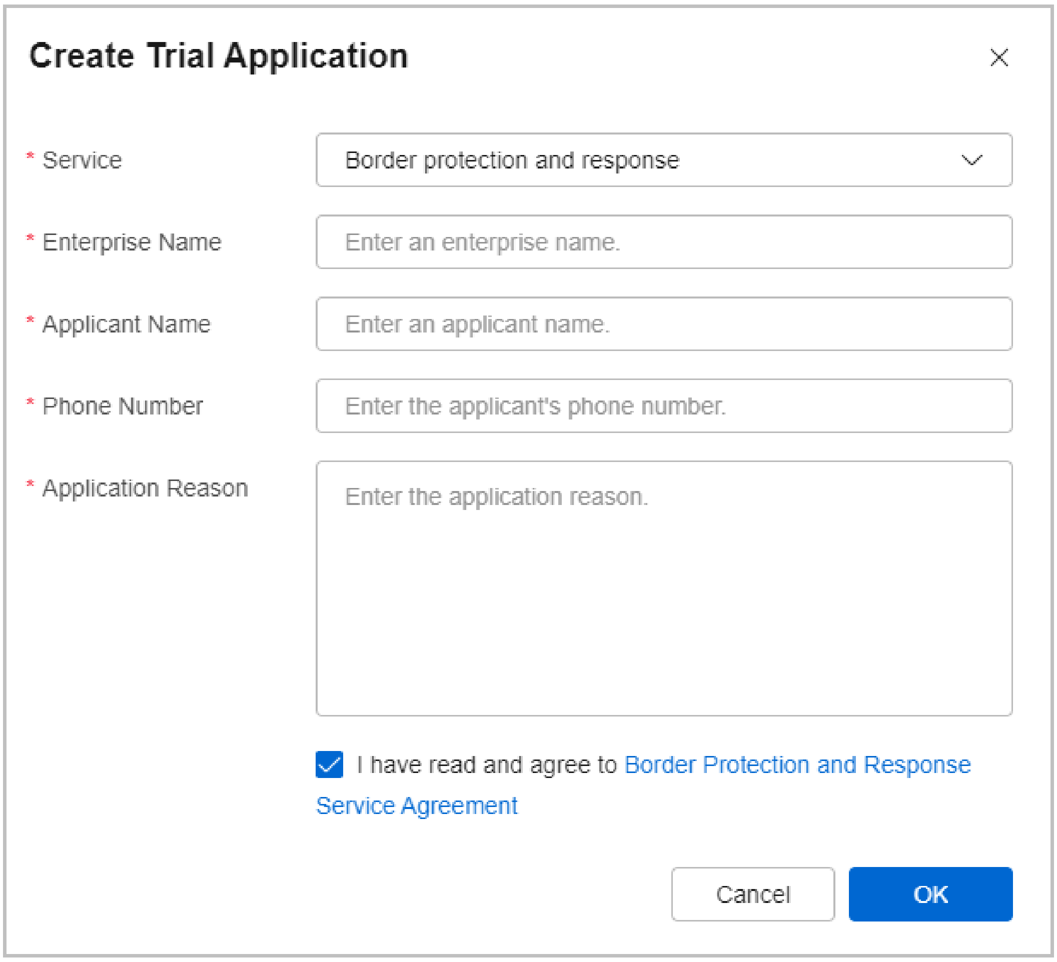
  NOTE

  The exported Excel file contains personal data, such as the username and user account. Please keep the file safe.

- Self-created tenants can be sorted by creation time. Click ⇅ behind **Creation At** in the list of self-created tenants to sort tenants by creation time.
- Modify self-created tenant information. Click **Modify** in the **Operation** column in the self-created tenant list to modify the tenant name, phone number, and email address.
- Apply for trial use on behalf of a tenant. Click **Apply for Free Trial** in the self-created tenant list, enter the trial product, enterprise name, contact person,

phone number, and application reason, and apply for one or more phones for the tenant. After the operations specialist approves the application, the tenant can enjoy the trial use.

Figure 10-6 Applying for trial use



Create Trial Application

* Service: Border protection and response

* Enterprise Name: Enter an enterprise name.

* Applicant Name: Enter an applicant name.

* Phone Number: Enter the applicant's phone number.

* Application Reason: Enter the application reason.

☑ I have read and agree to Border Protection and Response Service Agreement

- Change the initial password of an MSP-created account. Change the password immediately when using an MSP-created account to log in to the Huawei Qiankun **console** .. For details, see the *Tenant Operation Guide for Huawei Qiankun CloudService*.

11 Tenant Service Management

Prerequisites

You have logged in to the Huawei Qiankun console and have the permissions to manage specific services for tenants.

Context

MSPs can perform management and operations only on services authorized by tenants.

- **Tenant service management modes**

  The Huawei Qiankun console supports tenant service management from the service and tenant perspectives. You can flexibly select the management mode based on the service type and management habit.
- **Managed objects**

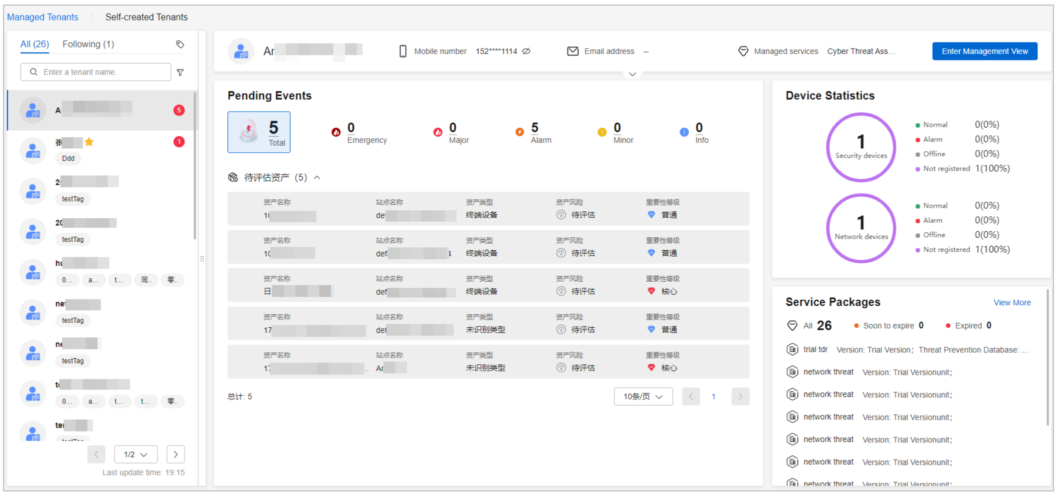
  The managed objects vary according to the managed services entrusted to an MSP. When managing the Border Protection and Response Service, the MSP needs to maintain the stable running of the software system, perform routine inspection, and handle emergencies of hardware devices.
- **Management metrics**

  Main focuses vary in terms of the product function, feature, status, and event of services managed by MSPs. Before managing a service, the MSP is recommended to learn and master the overall architecture and principles of the service to ensure an efficient and qualified management process.

Procedure

Step 1 Click **Tenants** in the upper right corner of the console. The **Managed Tenants** page is displayed by default.

Figure 11-1 Managed Tenants page


Managed Tenants
Self-created Tenants
All (26)
Following (1)
Enter a tenant name.
A[redacted] 5
张[redacted] ★ 1
Ddd
2[redacted]
testTag
20[redacted]
testTag
hu[redacted]
0... a... t... 同.. 零..
ne[redacted]
testTag
ne[redacted]
testTag
t[redacted]
0... a... t... t... 零..
te[redacted]
1/2
Last update time: 19:15
Ar[redacted]
Mobile number 152****1114
Email address --
Managed services Cyber Threat Ass...
Enter Management View
Pending Events
5 Total
0 Emergency
0 Major
5 Alarm
0 Minor
0 Info
待评估资产 (5)
资产名称 1[redacted] 站点名称 de[redacted] 资产类型 终端设备 资产风险 待评估 重要性等级 普通
资产名称 1[redacted] 站点名称 def[redacted] 资产类型 终端设备 资产风险 待评估 重要性等级 普通
资产名称 日[redacted] 站点名称 def[redacted] 资产类型 终端设备 资产风险 待评估 重要性等级 核心
资产名称 17[redacted] 站点名称 de[redacted] 资产类型 未识别类型 资产风险 待评估 重要性等级 普通
资产名称 1[redacted] 站点名称 Ar[redacted] 资产类型 未识别类型 资产风险 待评估 重要性等级 核心
总计: 5
10条/页
1
Device Statistics
1 Security devices
Normal 0(0%)
Alarm 0(0%)
Offline 0(0%)
Not registered 1(100%)
1 Network devices
Normal 0(0%)
Alarm 0(0%)
Offline 0(0%)
Not registered 1(100%)
Service Packages
View More
All 26
Soon to expire 0
Expired 0
trial tdr Version: Trial Version; Threat Prevention Database: ...
network threat Version: Trial Versionunit;
network threat Version: Trial Versionunit;
network threat Version: Trial Versionunit;
network threat Version: Trial Versionunit;
network threat Version: Trial Versionunit;
network threat Version: Trial Versionunit;

The following information is displayed:

- Tenant information: includes the name, phone number, and email address.
- Tenant list: displays the names and the number of pending events of all managed tenants.
  - After you click **Follow** next to a tenant name, the tenant is marked with a star in the list. To unfollow the tenant, click **Unfollow**.
  - After you click 🏷 next a username, you can add a label to the user on the **Add Label** page that is displayed. Then a labeled username is displayed in the list. You can click × next to the label to remove it as required.
- **Pending Events**: displays the number of pending events and basic event information. Select a pending event and click **One-Click Handling** to handle it. If the event does not need to be handled, you can click **Ignore**.

  NOTE

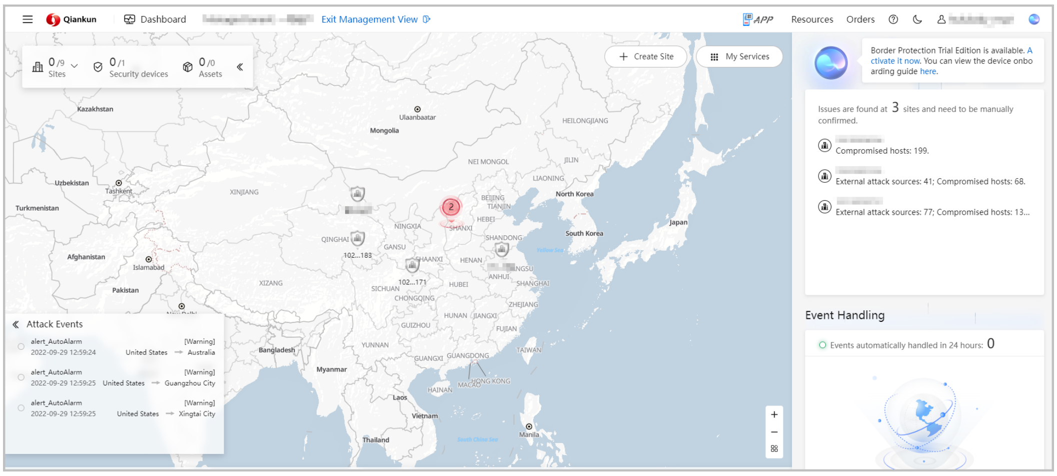
  Pending events that have been ignored will be reported later. Handle them in a timely manner.

- **Device Statistics**: include the number and status of devices.
- **Service Packages**: displays packages that are about to expire or have expired, so that MSPs can remind the managed tenants to renew the packages in a timely manner.

Step 2 Manage services for a tenant.

1. On the **Managed Tenants** page, select a tenant to be managed.
2. Click **Enter Management View**. The layout of the page for MSPs to maintain tenant services is similar to that for tenants to maintain their own services. For details, see **Homepage of the Console** under "Service Use" in the Tenant Operation Guide.
3. (Optional) Click ⌄ behind the name of a managed tenant. If you select another tenant from the drop-down list, the console homepage for this tenant is displayed. You can search for a tenant by entering its name in the search box.

Figure 11-2 Managed tenant page



Border Protection Trial Edition is available. Activate it now. You can view the device onboarding guide here.

Issues are found at 3 sites and need to be manually confirmed.

[redacted] Compromised hosts: 199.

[redacted] External attack sources: 41; Compromised hosts: 68.

[redacted] External attack sources: 77; Compromised hosts: 13...

Events automatically handled in 24 hours: 0

Attack Events

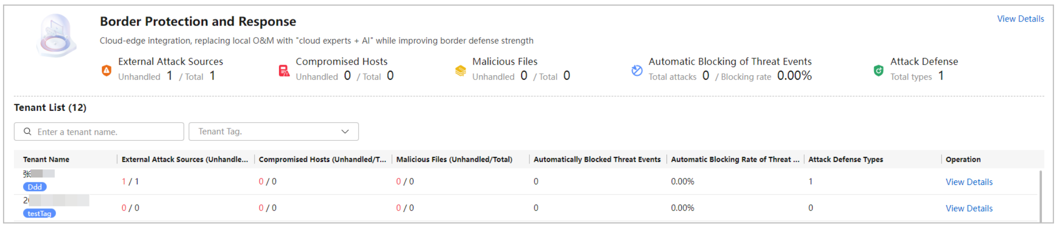
alert_AutoAlarm 2022-09-29 12:59:24	United States → Australia	[Warning]
alert_AutoAlarm 2022-09-29 12:59:25	United States → Guangzhou City	[Warning]
alert_AutoAlarm 2022-09-29 12:59:25	United States → Xingtai City	[Warning]

4. After the tenant management operations are complete, click **Exit Management View** in the upper part of the page.

Step 3 Perform operations on managed services.

Choose **Services** > **Border Protection and Response** in the upper right corner of the console. The managed service page is displayed.

Figure 11-3 Managed service page



Border Protection and Response

Cloud-edge integration, replacing local O&M with "cloud experts + AI" while improving border defense strength

View Details

External Attack Sources Unhandled 1 / Total 1

Compromised Hosts Unhandled 0 / Total 0

Malicious Files Unhandled 0 / Total 0

Automatic Blocking of Threat Events Total attacks 0 / Blocking rate 0.00%

Attack Defense Total types 1

Tenant List (12)

Enter a tenant name.

Tenant Tag.

Tenant Name	External Attack Sources (Unhandle...	Compromised Hosts (Unhandled/T...	Malicious Files (Unhandled/Total)	Automatically Blocked Threat Events	Automatic Blocking Rate of Threat ...	Attack Defense Types	Operation
张[redacted] Ddd	1 / 1	0 / 0	0 / 0	0	0.00%	1	View Details
2[redacted] testTag	0 / 0	0 / 0	0 / 0	0	0.00%	0	View Details

- In the upper part, an overview of managed services is displayed, including their key metrics (such as compromised hosts and external attack sources), facilitating quick detection of the overall service conditions. You can click **View Details** to view detailed information about the managed service of all tenants. Based on the information, you can evaluate service risks and handle exception events.
- In the lower part, a list of managed tenants is displayed, including their basic information and key metrics. You can click **View Details** in the **Operation** column of a tenant record to view detailed information about the tenant's service. You can search for a tenant by entering its name in the search box or by selecting a label. From this tenant list, you can quickly identify the tenants with high service risks and preferentially handle emergencies.

NOTE

The managed objects, O&M metrics, and tenant management operations vary according to the managed services entrusted to MSPs. For details, see the user guide of each service.

----End

12 Device Management

When an MSP is authorized to maintain tenant services, service resource management and maintenance are generally involved, especially device monitoring and management.

12.1 Managing Security Devices

Prerequisites

You have logged in to the Huawei Qiankun console and have the device management permission of the device lifecycle management service.

Context

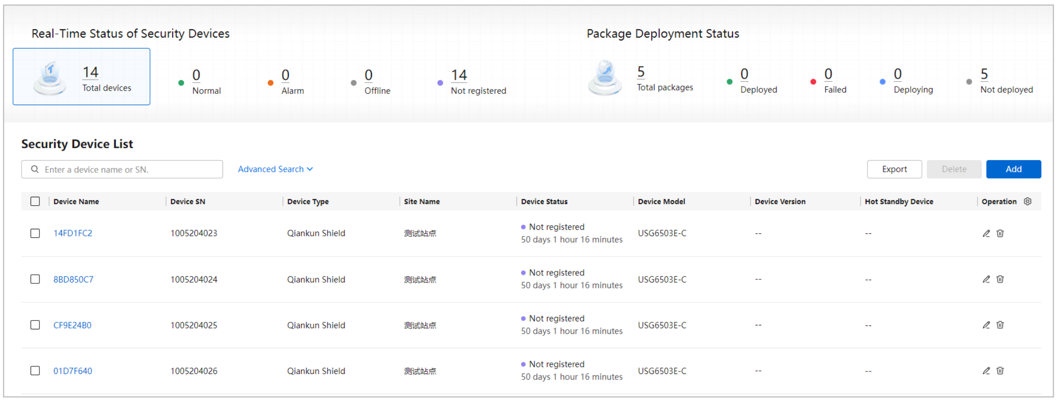
The security device management system is provided by Huawei Qiankun for MSPs to remotely monitor and manage security devices.

MSPs can quickly detect the running status and package deployment of managed security devices, implementing real-time remote monitoring and rapid emergency handling.

Procedure

Step 1 Choose **Security Devices** in the upper right corner of the console. The **Security Devices** page is displayed.

Figure 12-1 Security device management page



Real-Time Status of Security Devices

14 Total devices | 0 Normal | 0 Alarm | 0 Offline | 14 Not registered

Package Deployment Status

5 Total packages | 0 Deployed | 0 Failed | 0 Deploying | 5 Not deployed

Security Device List

Enter a device name or SN.

□	Device Name	Device SN	Device Type	Site Name	Device Status	Device Model	Device Version	Hot Standby Device	Operation
□	14FD1FC2	1005204023	Qiankun Shield	测试站点	Not registered 50 days 1 hour 16 minutes	USG6503E-C	--	--	
□	8BD850C7	1005204024	Qiankun Shield	测试站点	Not registered 50 days 1 hour 16 minutes	USG6503E-C	--	--	
□	CF9E24B0	1005204025	Qiankun Shield	测试站点	Not registered 50 days 1 hour 16 minutes	USG6503E-C	--	--	
□	01D7F640	1005204026	Qiankun Shield	测试站点	Not registered 50 days 1 hour 16 minutes	USG6503E-C	--	--	

- The security device overview is displayed in the upper part of the page.
  - **Real-Time Status of Security Devices**: displays the total number of security devices added by the current tenant and the distribution of devices in different states. **Table 12-1** describes the device states.

Table 12-1 Description of device states

Device State	Description	Possible Cause
Normal	A device is online.	N/A
Offline	A device is offline.	The network connectivity is abnormal or device configurations are lost.
Not registered	A device fails to go online.	The certificate expires, the network between the device and the Huawei Qiankun platform is disconnected, the device version or model is not supported, the registration service is not started, or IP address conflicts exist on the network.
	A device is invalid.	No device version information is available.
Alarm	A device is online and generates alarms.	The device configuration fails to be delivered, the CPU or memory usage of the device is high, a non-standard optical module is used on the device, or a network storm occurs.

NOTE

If a device is invalid, delete the device and add it again.

  - **Package Deployment Status**: displays the deployment states of packages for all security devices, as described in **Table 12-2**.

Table 12-2 Description of package deployment states

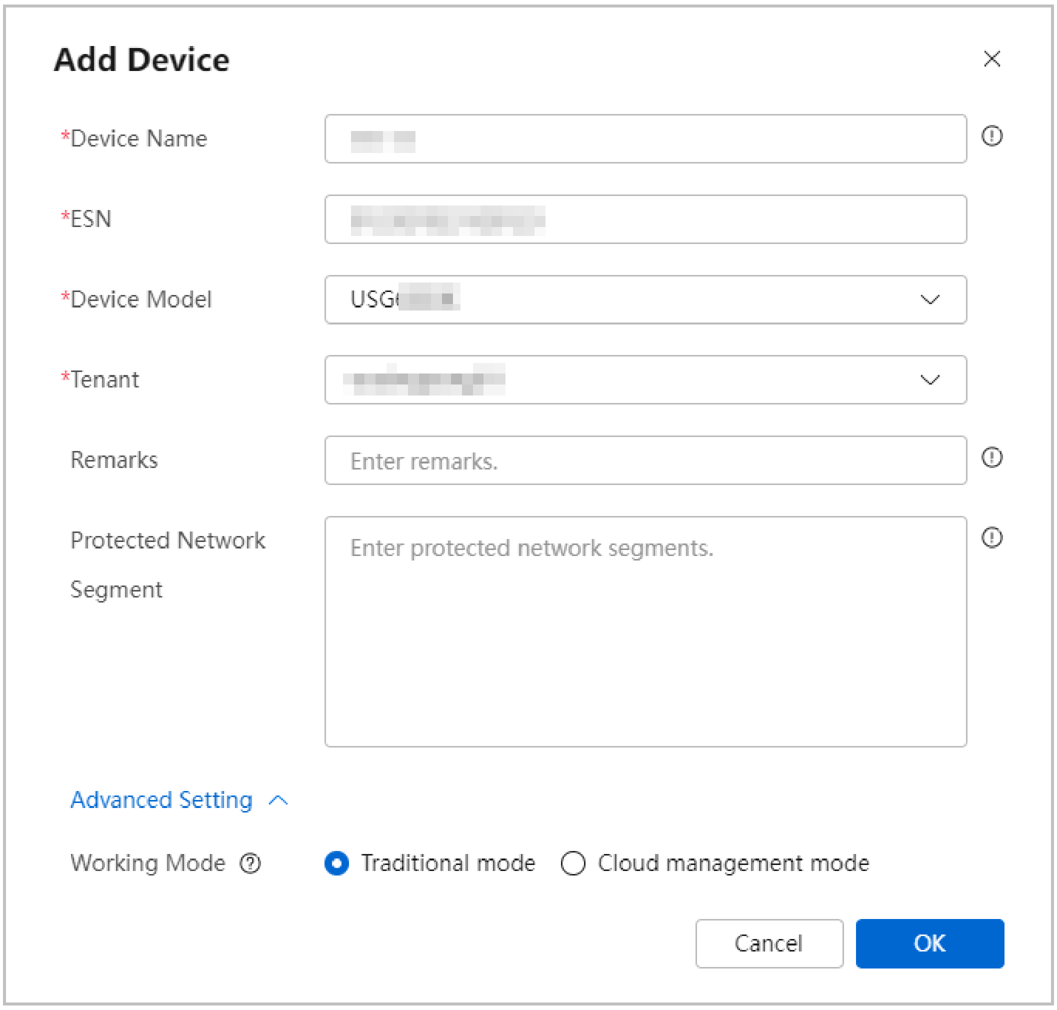
Package State	Description
Deployed	After a device goes online, the package is successfully activated and configurations are successfully delivered to the device.
Failed	After a device goes online, the package fails to be activated or configurations fail to be delivered to the device.
Deploying	After a device goes online, the package is being activated and configurations are being delivered.
Not deployed	The device is not online, the package is not activated, and configurations are not delivered.

- The security device list is displayed in the lower part of the page. The device information includes the device name, device SN, home tenant, home site, bypass function status, and working mode.

Step 2 Add a security device.

Click **Add**, enter related information based on **Table 12-3**, and click **OK**.

Figure 12-2 Adding a security device



Add Device

*Device Name [redacted]

*ESN [redacted]

*Device Model USG[redacted]

*Tenant [redacted]

Remarks Enter remarks.

Protected Network Segment Enter protected network segments.

Advanced Setting

Working Mode ● Traditional mode ○ Cloud management mode

Table 12-3 Description of security device parameters

Parameter	Description
Device Name	Name of a security device. The value can contain only letters, digits, and special characters (excluding spaces).
SN	Equipment serial number, which uniquely identifies a device.
Device Model	Currently, USG6603F-C and USG6000E series firewalls are supported.
Tenant	Managed tenant to which a managed security device belongs.
Protected Network Segment	Network segments to be protected. You can configure multiple protected network segments separated by carriage return characters. For example: 10.0.0.0/11 10.0.0.0-10.31.255.255

Parameter	Description
Working Mode	● Traditional mode (default): You need to log in to the device to complete network configurations. ● Cloud management mode: You can complete basic network configurations for the device on the console.

Step 3 Export the security device list.

Click **Export** to export the current security device list.

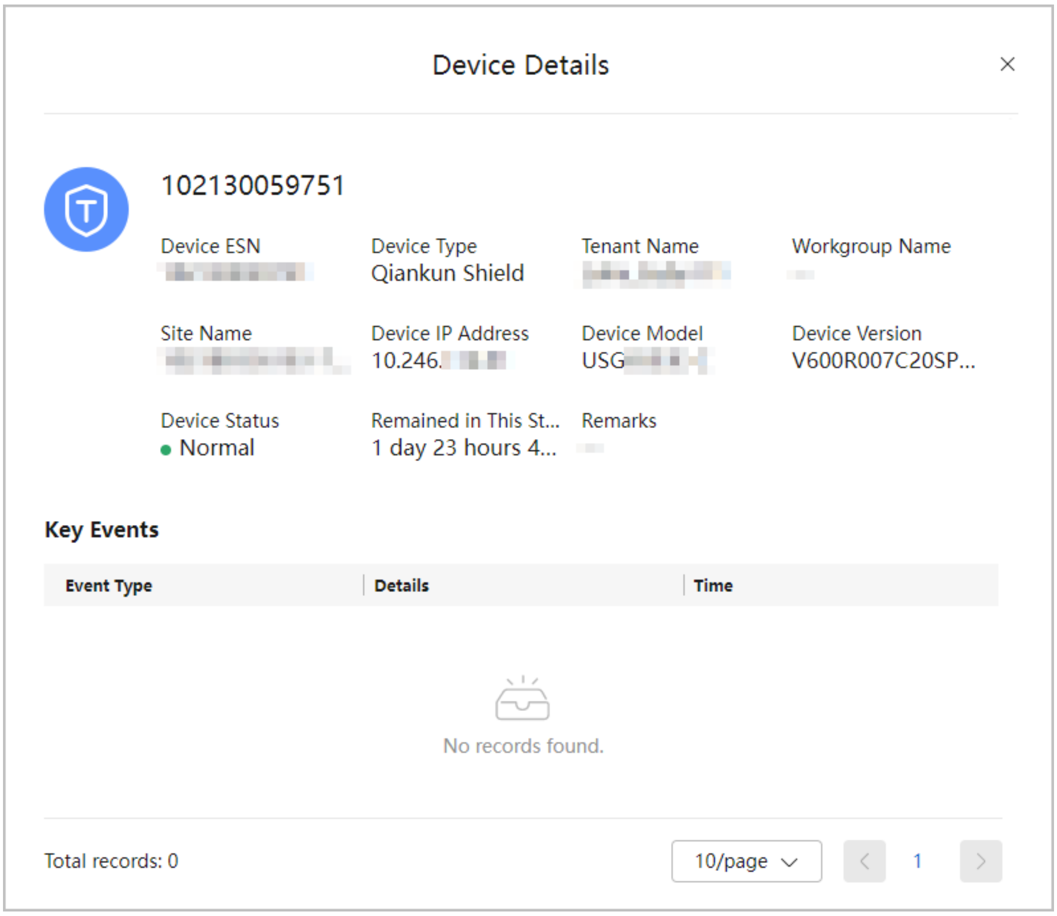
NOTE

A maximum of 10,000 device data records can be exported. If the exported CSV file contains fields starting with special characters @ - + =, CSV injection risks may exist.

Step 4 View security device details.

Click a security device name. The **Device Details** page is displayed on the right, showing device information such as the device name, CPU and memory usage, interface outbound rate, and interface inbound rate.

Figure 12-3 Device Details page



Device Details

102130059751

Device ESN
[redacted]

Device Type
Qiankun Shield

Tenant Name
[redacted]

Workgroup Name
[redacted]

Site Name
[redacted]

Device IP Address
10.246.[redacted]

Device Model
USG[redacted]

Device Version
V600R007C20SP...

Device Status
● Normal

Remained in This St...
1 day 23 hours 4...

Remarks
[redacted]

Key Events

Event Type	Details	Time

No records found.

Total records: 0

10/page

1

Step 5 Perform operations on security devices. You can search for, edit, and delete security devices, bind hot standby devices to them, and configure the bypass function. **Table 12-4** describes these operations in detail.

Table 12-4 Operations that can be performed on security devices

Operation	Description
Search	● Search by keyword: Enter a device name or SN in the search box, and click 🔍 or press **Enter**. ● Advanced search: Click **Advanced Search**, and enter search criteria including the tenant name, device status, and device type.
Edit	Select a security device, click ✎ in the security device list, and modify the device name.
Delete	Select a security device, and click 🗑 in the **Operation** column or **Delete** to delete the security device. After a device is deleted, you cannot handle the events detected by it. Exercise caution when performing this operation.
Remote login	Select a security device, click 🖥 in the list, enter the management view, and log in to the device remotely. **NOTE** Only devices whose statuses are **Normal** or **Alarm** support the remote login function.

----End

13 Service Ticket Management

13.1 Creating a Service Ticket

Prerequisites

You have logged in to the Huawei Qiankun console and have the permission to manage service tickets.

Context

Huawei Qiankun provides the service ticket function for issue handling and tracking.

When using Huawei Qiankun, an MSP can create service tickets if the MSP encounters any problems. After receiving the service tickets, Huawei Qiankun engineers will quickly analyze, locate, and resolve the problems.

Based on the service ticket change, the MSP can learn about its processing progress, thereby ensuring the stable running of managed services.

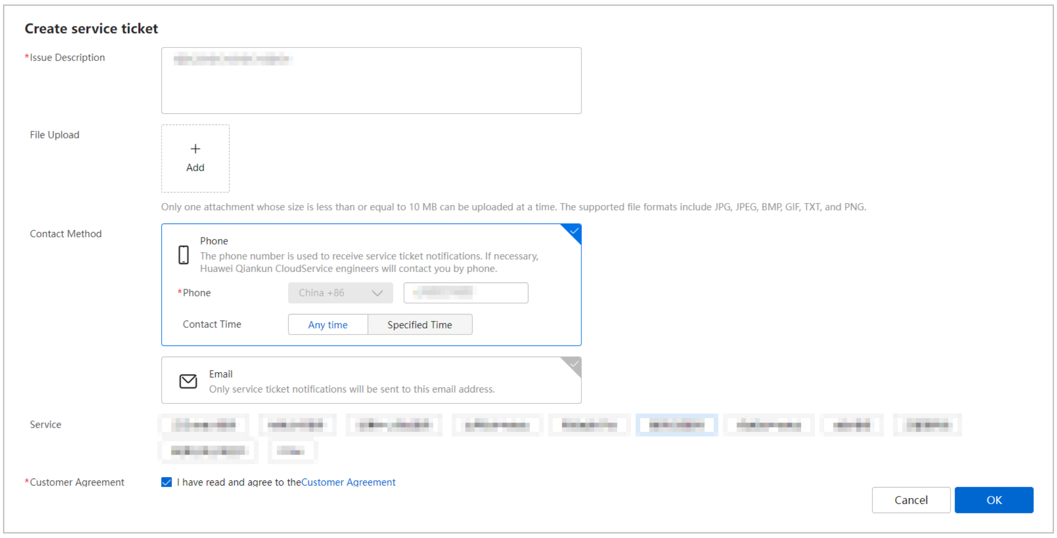
Procedure

Step 1 Log in to the console, click your account in the upper right corner, and choose **Service Tickets** > **My Service Tickets**.

Step 2 Create a service ticket.

Click **Create**, and enter related information. **Table 13-1** describes the parameters.

Figure 13-1 Creating a service ticket



Create service ticket

*Issue Description [redacted]

File Upload

+ Add

Only one attachment whose size is less than or equal to 10 MB can be uploaded at a time. The supported file formats include JPG, JPEG, BMP, GIF, TXT, and PNG.

Contact Method

Phone
The phone number is used to receive service ticket notifications. If necessary, Huawei Qiankun CloudService engineers will contact you by phone.

*Phone China +86 [redacted]

Contact Time [✓ Any time] Specified Time

Email
Only service ticket notifications will be sent to this email address.

Service [redacted]

*Customer Agreement ☑ I have read and agree to theCustomer Agreement

Cancel OK

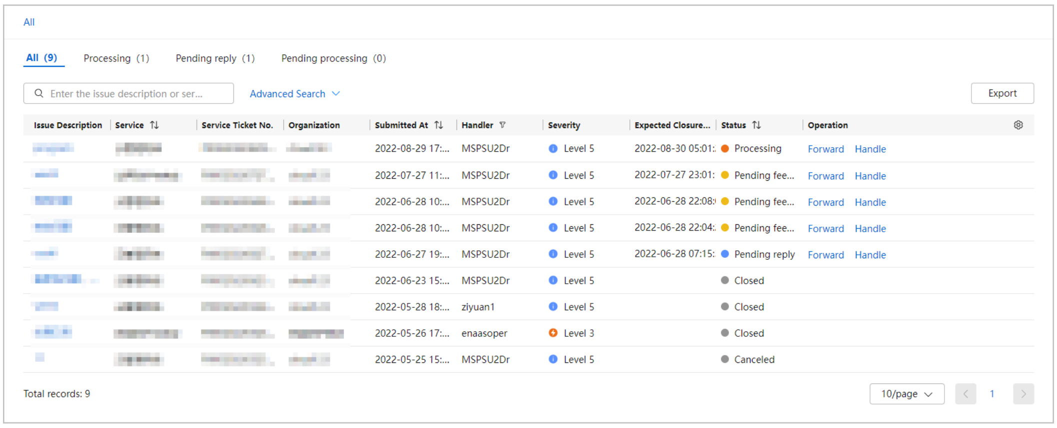
Table 13-1 Parameters for creating a service ticket

Parameter	Description
Service	Service for which a service ticket is to be submitted. If the desired service is not found in the service list, contact Huawei Qiankun engineers at sa@huawei.com.
Issue Type	Type of the issue you want to report in the service ticket.
Issue Description	Issue description in text or images. For example, you can describe the abnormal device status or exceptions occurring during yours operations. Do not enter your confidential information such as your username, password, and bank account.
File Upload	You can upload a maximum of five local files for supplementary description. Only files in JPG, JPEG, BMP, GIF, TXT, and PNG formats are supported.
Contact Method	By default, **In-ticket messages** is used to track service ticket processing. You can also select **Phone** or **Email**, or both of them. If you select **Phone**, you can set **Contact Time** to a specified period of time.

Step 3 View service ticket details.

The **My Service Tickets** page consists of three major parts: service ticket overview, service ticket search, and service ticket list.

Figure 13-2 My Service Tickets page



Issue Description	Service	Service Ticket No.	Organization	Submitted At	Handler	Severity	Expected Closure...	Status	Operation
[redacted]	[redacted]	[redacted]	[redacted]	2022-08-29 17:...	MSPSU2Dr	Level 5	2022-08-30 05:01:	Processing	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-07-27 11:...	MSPSU2Dr	Level 5	2022-07-27 23:01:	Pending fee...	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-28 10:...	MSPSU2Dr	Level 5	2022-06-28 22:08:	Pending fee...	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-28 10:...	MSPSU2Dr	Level 5	2022-06-28 22:04:	Pending fee...	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-27 19:...	MSPSU2Dr	Level 5	2022-06-28 07:15:	Pending reply	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-23 15:...	MSPSU2Dr	Level 5		Closed	
[redacted]	[redacted]	[redacted]	[redacted]	2022-05-28 18:...	ziyuan1	Level 5		Closed	
[redacted]	[redacted]	[redacted]	[redacted]	2022-05-26 17:...	enaasoper	Level 3		Closed	
[redacted]	[redacted]	[redacted]	[redacted]	2022-05-25 15:...	MSPSU2Dr	Level 5		Canceled	

Total records: 9

- Service ticket overview

  Click **All**, **Dispatching**, **Processing**, or **Pending Confirmation** in the upper part of the page to filter the service tickets in the respective states.

- Service ticket search

  - Search by keyword: Enter a keyword, and click 🔍 or press **Enter**.
  - Advanced search: Click **Advanced Search**, select search criteria, and click **Search**.

    The search criteria change according to your selection in the service ticket overview area, as described in Table 13-2. Table 13-3 describes the service ticket states.

Table 13-2 Search criteria

Selection in the Service Ticket Overview Area	Search Criteria
All	Service, service ticket state, and submission time
Dispatching, Processing, or Pending Confirmation	Service and submission time

Table 13-3 Service ticket states

Service Ticket State	Description
Dispatching	The system is dispatching a service ticket to a Huawei Qiankun engineer.
Processing	A Huawei Qiankun engineer has received a service ticket and is handling the issue.

Service Ticket State	Description
Pending Confirmation	A Huawei Qiankun engineer has handled the service ticket and waits for your confirmation and evaluation.
Canceled	You have canceled a service ticket in dispatching state. Canceled service tickets do not need to be processed by Huawei Qiankun engineers.
Closed	A service ticket has been closed. If you have any other problems, you need to create another service ticket.

- Service ticket list

  The list records service ticket information such as the service, issue type, No., time, and state. You can perform various operations on service tickets, as described in **Table 13-4**.

Table 13-4 Operations that can be performed on service tickets

Operation	Description
Send a reminder	Click **Send Reminder** in the **Operation** column. When receiving your reminder, the corresponding Huawei Qiankun engineer will process the service ticket as soon as possible.
Cancel	For a service ticket in dispatching state, you can click **Cancel** in the **Operation** column to cancel it.
Leave messages	– On the message leaving page, you can directly communicate with Huawei Qiankun engineers via messages or images. You can also recall a message and edit it again within two minutes after the message is sent. – On the message leaving page, you can send a reminder, and cancel or close the service ticket. – On the message leaving page, you can view service ticket processing logs about the create, process, close, and other operations.
Review	Give your review and rating after the engineer completes processing your service ticket.
Delete	For a service ticket in canceled or closed state, you can click **Delete** in the **Operation** column to delete it. **CAUTION** Exercise caution when performing this operation because a service ticket cannot be restored after being restored.

Operation	Description
Export	Click **Export**, read the message in the displayed dialog box, and click **OK**. **NOTE** The exported Excel file contains the issue type, service name, service ticket state, and phone number or email address. Keep the file safe as it involves personal data.

- Service ticket authorization

  When Huawei Qiankun engineers process service tickets, they may require some information from you for fault locating. To obtain such information, Huawei Qiankun engineers must obtain formal authorization from you. Authorization information includes:

  – Confidential information, such as usernames and passwords for logging in to devices

  – Statement of commitment, which needs to be signed by you

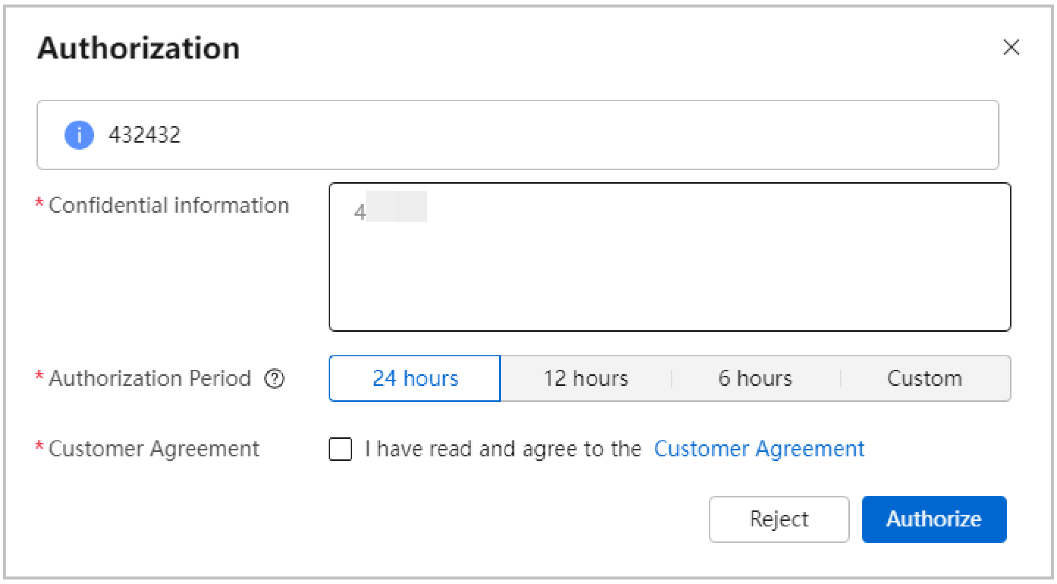
  NOTE

  Carefully check the authorization information to be provided. If you have any questions, contact Huawei Qiankun engineers by leaving messages.

  You can process authorization requests using either of the following methods:

  – In the chat window, click **Authorize** as prompted. For details, see **Table 13-5**.

Figure 13-3 Service ticket authorization



Authorization

432432

* Confidential information: 4

* Authorization Period: 24 hours | 12 hours | 6 hours | Custom

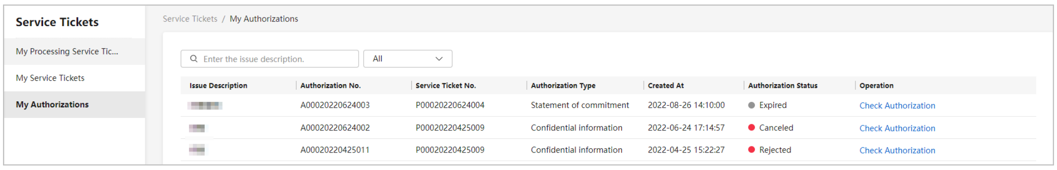
* Customer Agreement: □ I have read and agree to the Customer Agreement

Table 13-5 Operations related to service ticket authorization

Operation	Description
Reply	■ For confidential information, provide it in the text box. ■ For statement of commitment, read it carefully. No reply is required.
Set an authorization period	When the authorization period expires, the system automatically clears the authorized information, and Huawei Qiankun engineers can no longer view the information. In this case, you are advised to modify the authorized information right away.
Sign the Customer Agreement	Read and sign the Customer Agreement before authorizing the required information.
Accept or reject the authorization request	■ To accept the authorization request, click **Authorize**. ■ To reject the authorization request, click **Reject**. **NOTE** To cancel the authorization, click **Cancel Authorization**.

– On the **Service Tickets** page, choose **My Authorizations** from the navigation tree. Select the target service ticket, click **Authorize** in the **Operation** column, and perform operations by referring to **Table 13-5**.

Figure 13-4 My Authorizations page


Service Tickets
My Processing Service Tic...
My Service Tickets
My Authorizations
Service Tickets / My Authorizations
Enter the issue description.
All

Issue Description	Authorization No.	Service Ticket No.	Authorization Type	Created At	Authorization Status	Operation
[redacted]	A00020220624003	P00020220624004	Statement of commitment	2022-08-26 14:10:00	● Expired	Check Authorization
[redacted]	A00020220624002	P00020220425009	Confidential information	2022-06-24 17:14:57	● Canceled	Check Authorization
[redacted]	A00020220425011	P00020220425009	Confidential information	2022-04-25 15:22:27	● Rejected	Check Authorization

You can view historical authorization records on the **My Authorizations** page.

----End

13.2 Processing a Service Ticket

Prerequisites

You have logged in to the Huawei Qiankun console and have the permission to manage service tickets.

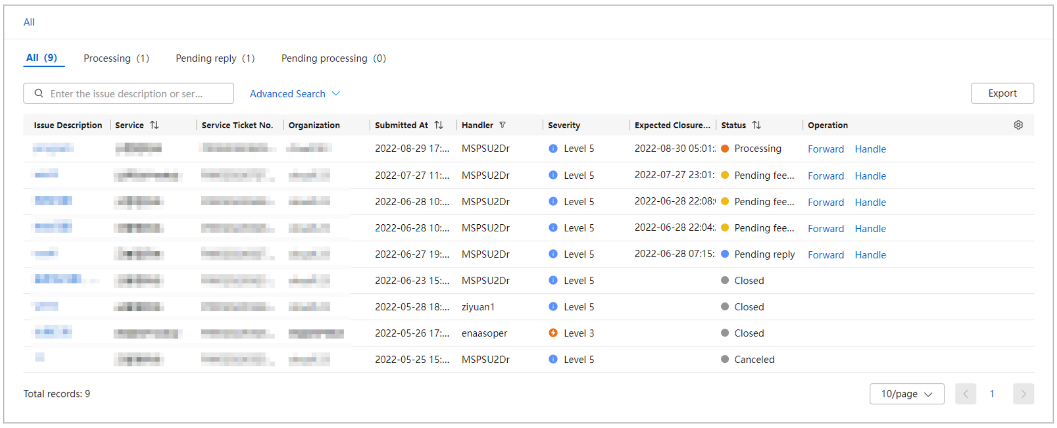
Context

After a site reliability engineer (SRE) of Huawei Qiankun assigns service tickets to an MSP, the MSP has the permissions for processing all service tickets of managed tenants.

Procedure

1. Click **Service Tickets** in the menu bar. The **My Service Tickets** page is displayed.
2. Choose **My Processing Service Tickets** to view the service tickets to be processed.

Figure 13-5 Service ticket list

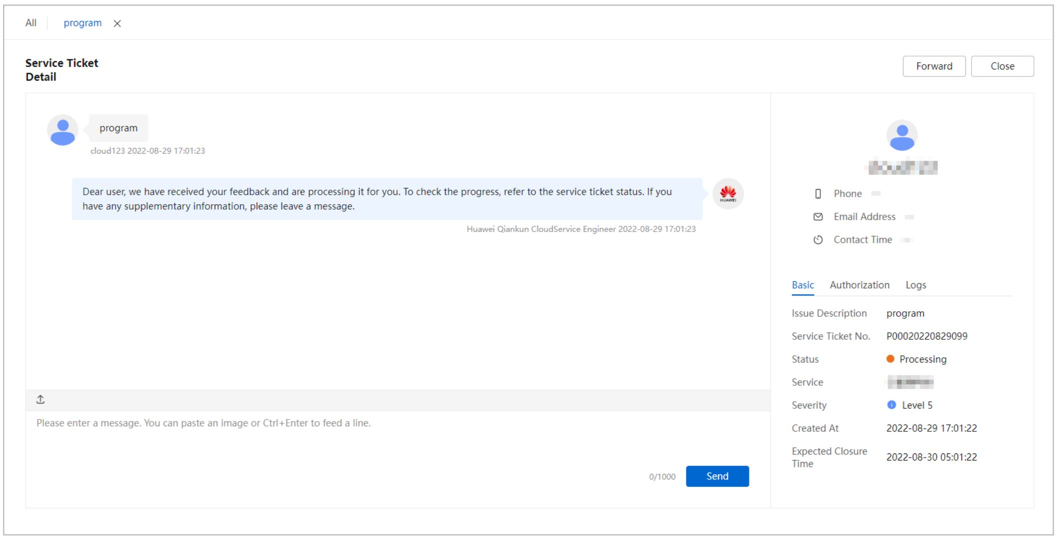


Issue Description	Service	Service Ticket No.	Organization	Submitted At	Handler	Severity	Expected Closure...	Status	Operation
[redacted]	[redacted]	[redacted]	[redacted]	2022-08-29 17:...	MSPSU2Dr	Level 5	2022-08-30 05:01:	● Processing	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-07-27 11:...	MSPSU2Dr	Level 5	2022-07-27 23:01:	● Pending fee...	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-28 10:...	MSPSU2Dr	Level 5	2022-06-28 22:08:	● Pending fee...	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-28 10:...	MSPSU2Dr	Level 5	2022-06-28 22:04:	● Pending fee...	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-27 19:...	MSPSU2Dr	Level 5	2022-06-28 07:15:	● Pending reply	Forward Handle
[redacted]	[redacted]	[redacted]	[redacted]	2022-06-23 15:...	MSPSU2Dr	Level 5		● Closed	
[redacted]	[redacted]	[redacted]	[redacted]	2022-05-28 18:...	ziyuan1	Level 5		● Closed	
[redacted]	[redacted]	[redacted]	[redacted]	2022-05-26 17:...	enaasoper	Level 3		● Closed	
[redacted]	[redacted]	[redacted]	[redacted]	2022-05-25 15:...	MSPSU2Dr	Level 5		● Canceled	

Total records: 9

3. Select a service ticket to be processed from the list. Click the service ticket name in the **Issue Description** column or click **Handle**. The service ticket processing page is displayed.

Figure 13-6 Processing a service ticket



program

cloud123 2022-08-29 17:01:23

Dear user, we have received your feedback and are processing it for you. To check the progress, refer to the service ticket status. If you have any supplementary information, please leave a message.

Huawei Qiankun CloudService Engineer 2022-08-29 17:01:23

Please enter a message. You can paste an image or Ctrl+Enter to feed a line.

0/1000

[redacted]

Phone [redacted]

Email Address [redacted]

Contact Time [redacted]

Issue Description	program
Service Ticket No.	P00020220829099
Status	● Processing
Service	[redacted]
Severity	Level 5
Created At	2022-08-29 17:01:22
Expected Closure Time	2022-08-30 05:01:22

On the service ticket processing page, you can view **Issue Description** and **Status** of a service ticket, and modify service ticket information.

- **Issue Description**

  Description entered when the service ticket is submitted.

- **Status**

  State of a service ticket. For details, see **Table 13-6**.

Table 13-6 Service ticket states

Service Ticket State	Description
Processing	An MSP administrator has received a service ticket and is handling the issue.
Pending feedback	An MSP administrator has sent a message to you and waits for a reply.
Pending confirmation	An MSP administrator has handled the service ticket and waits for your confirmation and evaluation.
Pending reply	You have sent a message and wait for a reply from an MSP administrator.
Canceled	You have canceled a service ticket in dispatching state. Canceled service tickets do not need to be processed by MSP administrators.
Closed	A service ticket has been closed. If you have any other problems, you need to create another service ticket.

- Severity

  Service ticket severities are the grading standards defined by the operations personnel for differentiating service requests. Service tickets in different severities are expected to be resolved at different time. An MSP administrator does not have the permission to change the service ticket severity.

Table 13-7 Service ticket severity

Severity	Definition	Required Resolution Time
Severity 1	Core production system unavailable	Must be resolved or escalated within 15 minutes
Severity 2	Production system partially unavailable	Must be resolved or escalated within 30 minutes

Severity	Definition	Required Resolution Time
Severity 3	Production system exception	Must be resolved or escalated within 1 hour
Severity 4	System exception	Must be resolved or escalated within 6 hours
Severity 5	General guidance	Must be resolved or escalated within 12 hours

4. Further process the service ticket.
   - **Forward**: For a problem that cannot be solved or should not be handled by an MSP administrator, click **Forward** to transfer the service ticket back to the SRE.
   - **Close**: For a service ticket that has been processed, click **Close** and wait for the confirmation and feedback.

     NOTE

     If you report that a service ticket has been resolved, the service ticket is automatically closed.

     If you report that a service ticket is not resolved, the service ticket needs to be followed and resolved.

14 Package Management

Prerequisites

You have logged in to the Huawei Qiankun console.

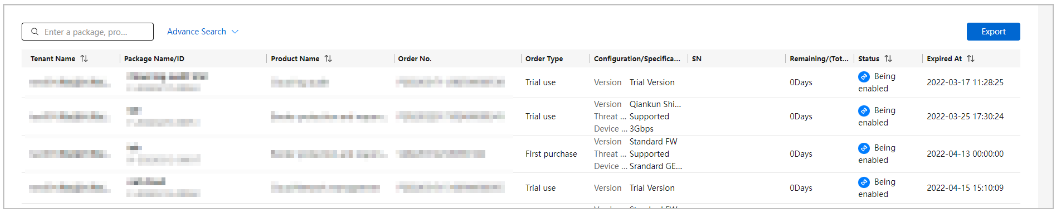
Context

Through package management, MSP administrators can comprehensively understand the package state of each managed tenant.

Procedure

1. Choose **Operations** > **Packages** in the upper right corner of the console. The **Packages** page is displayed.

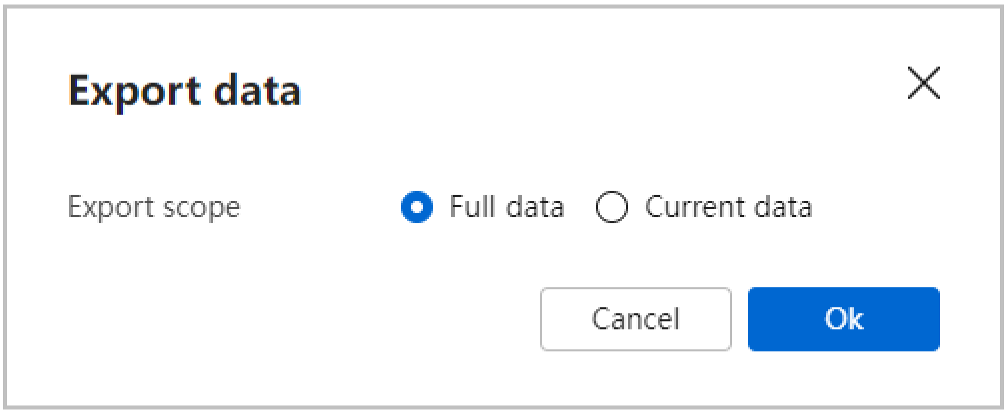
Figure 14-1 Managing a package



Tenant Name	Package Name/ID	Product Name	Order No.	Order Type	Configuration/Specifica...	SN	Remaining/(Tot...	Status	Expired At
[redacted]	[redacted]	[redacted]	[redacted]	Trial use	Version Trial Version		0Days	Being enabled	2022-03-17 11:28:25
[redacted]	[redacted]	[redacted]	[redacted]	Trial use	Version Qiankun Shi... Threat ... Supported Device ... 3Gbps		0Days	Being enabled	2022-03-25 17:30:24
[redacted]	[redacted]	[redacted]	[redacted]	First purchase	Version Standard FW Threat ... Supported Device ... Srandard GE...		0Days	Being enabled	2022-04-13 00:00:00
[redacted]	[redacted]	[redacted]	[redacted]	Trial use	Version Trial Version		0Days	Being enabled	2022-04-15 15:10:09

2. Search for packages.
   - Search by keyword: Enter a package name, product name, or tenant name and click 🔍 or press **Enter**.
   - Advanced search: Click **Advanced Search** and search for packages by package name, product name, tenant name, package state, and package expiration time.
3. Click **Export** in the upper right corner of the package list, select the export scope, and click **OK** to export data.

Figure 14-2 Exporting data



Export data

Export scope ● Full data ○ Current data

15 Log Viewing

Prerequisites

You have logged in to the Huawei Qiankun console and have the cloud log audit service permission.

Context

Huawei Qiankun provides logs to help you quickly learn about the service running status and historical operations.

Currently, the console supports operation logs and security logs.

- Operation logs record a variety of user operations such as subscribing to topics, creating service tickets, and managing devices.
- Security logs record security-related information, such as user login and lower-level workgroup account creation.
- You can view logs generated in the last six months on the console. To view logs generated in the past 6–12 months, download them to your local PC.

A log contains information such as the operation name, operation object, operation result, and severity.

Procedure

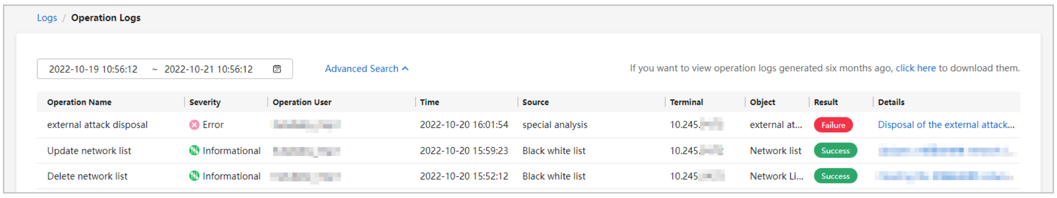
Step 1 Click your account in the upper right corner of the console, and choose **Logs**.

Step 2 View, search for, and download logs. The following uses operation logs as an example. The operations that can be performed on security logs are similar.

1. View the log list.

   On the **Operation Logs** page, view log information such as the name, object, and result of each operation.

Figure 15-1 Log list



Logs / Operation Logs

2022-10-19 10:56:12 ~ 2022-10-21 10:56:12

Advanced Search

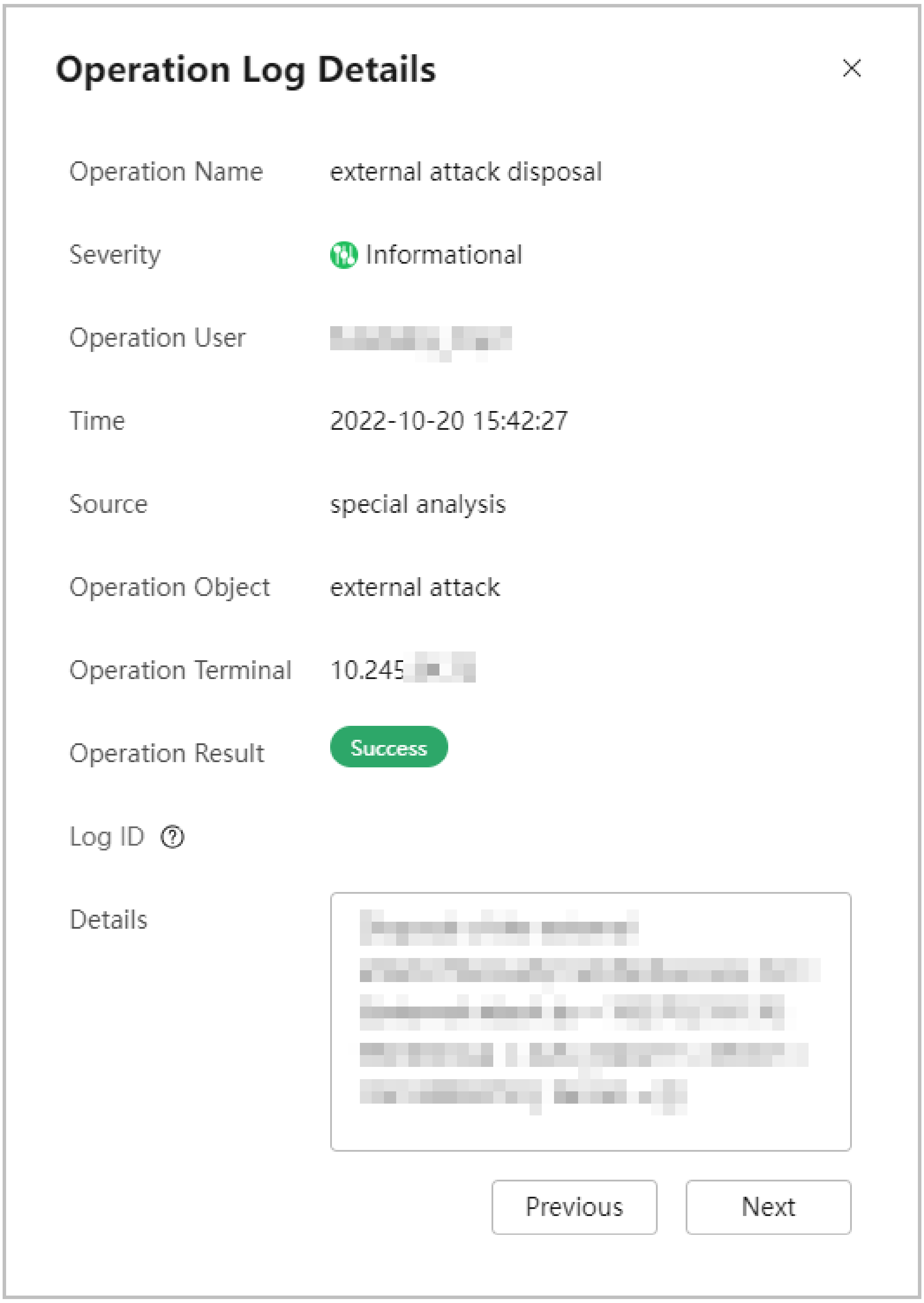
If you want to view operation logs generated six months ago, click here to download them.

Operation Name	Severity	Operation User	Time	Source	Terminal	Object	Result	Details
external attack disposal	Error	[redacted]	2022-10-20 16:01:54	special analysis	10.245.[redacted]	external at...	Failure	Disposal of the external attack...
Update network list	Informational	[redacted]	2022-10-20 15:59:23	Black white list	10.245.[redacted]	Network list	Success	[redacted]
Delete network list	Informational	[redacted]	2022-10-20 15:52:12	Black white list	10.245[redacted]	Network Li...	Success	[redacted]

2. View log details.

   Click any item in the **Details** column of a log to view log details.

   Figure 15-2 Log details

   Operation Log Details

   Operation Name: external attack disposal

   Severity: Informational

   Operation User: [redacted]

   Time: 2022-10-20 15:42:27

   Source: special analysis

   Operation Object: external attack

   Operation Terminal: 10.245[redacted]

   Operation Result: Success

   Log ID

   Details: [redacted]

3. Search for logs.

   Click **Advanced Search**, set search criteria based on **Table 15-1**, and click **Search**.

Table 15-1 Search criteria

Parameter	Description
Time	Set the start time and end time to display logs generated in the specified period.
Severity	Select log severity levels. The options include: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, and **Debug**, which are listed in descending order of severity.
Operation Result	The log operation result can be **Success**, **Failure**, and **Partial success**.

📖 NOTE

You can click **Reset** to restore the search criteria to the default settings:

- Records in the last 48 hours
- All log severity levels
- All operation results

4. Download logs.

   You can view logs generated in the last six months on the console. To view logs generated in the past 6–12 months, click **click hear** in the upper right corner to download the logs.

----End

16 Download Center

Prerequisites

You have logged in to the Huawei Qiankun console.

Context

Huawei Qiankun provides a download center to help you centrally manage file downloads.

Currently, the system supports file download only for the Border Protection and Response Service.

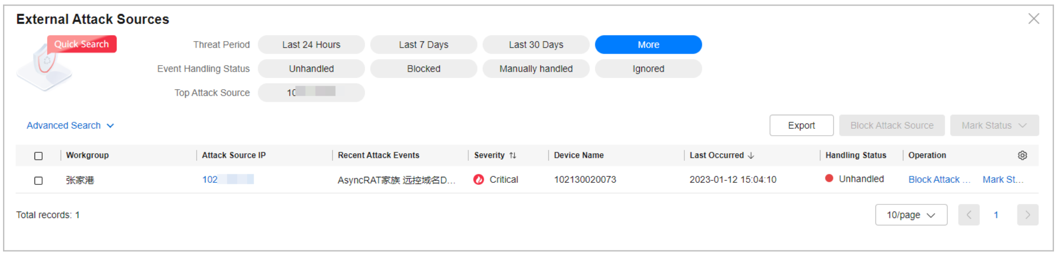
- The download center can store only the latest 30 records. Earlier records that exceed this will be automatically deleted. Therefore, delete unnecessary files in a timely manner.
- File download operations are recorded in security logs.

Procedure

1. On the console homepage, choose **Services** > **Border Protection and Response**.
2. View the threat event overview.
   - Click **View Details** in the upper right corner of the page to view the threat event overview of all existing tenants under the current MSP account.
   - Click **View Details** in the **Operation** column in the tenant list to view the threat event overview of an existing tenant.
3. Download the threat event information. You can export the information about threat event overview, external attack sources, compromised hosts, and malicious files.

   Click **View More** in the upper right corner of a card, and click **Export** in the displayed dialog box.

Figure 16-1 Exporting event details



External Attack Sources

Threat Period: Last 24 Hours | Last 7 Days | Last 30 Days | More

Event Handling Status: Unhandled | Blocked | Manually handled | Ignored

Top Attack Source: 10[redacted]

□	Workgroup	Attack Source IP	Recent Attack Events	Severity	Device Name	Last Occurred	Handling Status	Operation
□	张家港	102[redacted]	AsyncRAT家族 远控域名D...	Critical	102130020073	2023-01-12 15:04:10	● Unhandled	Block Attack ... Mark St...

Total records: 1

4. Click your account in the upper right corner of the console, and click **Download Center**. Then click **Download** in **Operation** column to download a file.

   NOTE

   The download center can store only a maximum of 30 records. If the number of stored records reaches the upper limit, the earliest records will be automatically overwritten based on the export time. Therefore, delete unnecessary files in a timely manner.

Follow-up Procedure

- Searching for files: In the download center, enter a file name in the search box, and click 🔍 or press **Enter**.
- Deleting files:
  - Deleting a single file: In the download center, select a file to be deleted in the list and click **Delete**.
  - Deleting files in batches: In the download center, select files to be deleted and click **Delete** above the list.

17 Message Center

Prerequisites

You have logged in to the Huawei Qiankun console.

Context

Huawei Qiankun provides a message center to help you centrally manage messages.

📖 NOTE

Currently, only the **admin** user can configure message types, including the message type name and whether to support emails, SMS messages, and system messages.

Procedure

1. Click your account in the upper right corner of the console, and click **Message Center**.
2. View system messages.

   On the **Message Center** page, choose **My Messages**.

   a. On the **My Messages** page, you can view all messages or unread messages.

   b. On the **My Messages** page, you can filter messages by message type or by entering a message name in the search box.

   c. Select a message, and click **Operation** to mark the message as read or delete the message.
3. Configure message receiving.

   Choose **Message Receiving Management** > **SMS & Email Settings** from the navigation tree.

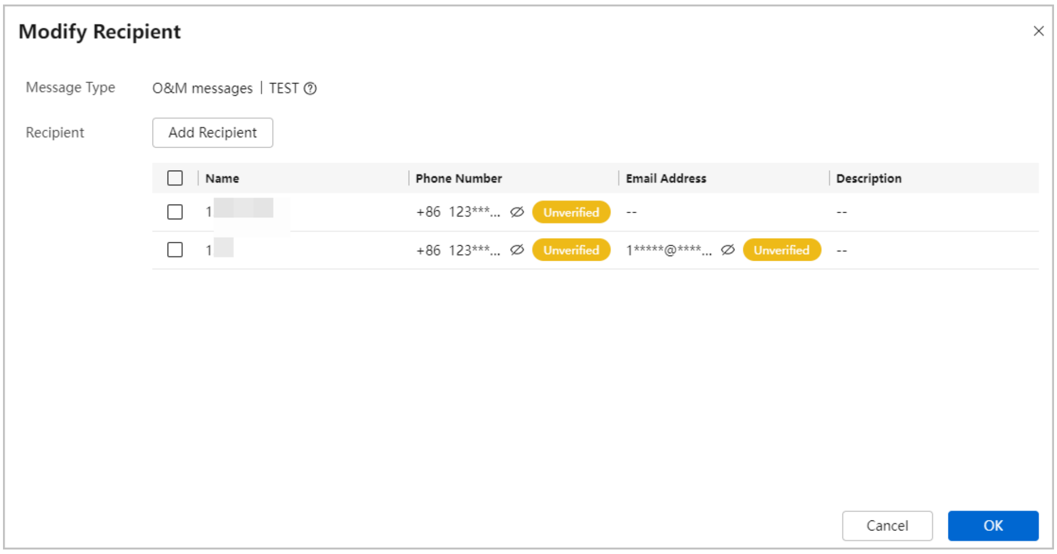
   a. Set the message receiving mode. Currently, messages can be received via system message, email, and SMS. You can select or deselect the check box of a message receiving mode to configure it.

   b. Preview the message template. Click **Preview** in the **Operation** column to view the current message template.

c. Modify a recipient. Click **Modify Recipient** in the **Operation** column to add a recipient for the current message or modify the recipient information.

If there is no recipient, you can click **Add Recipient** to add one.

Figure 17-1 Modifying a recipient



Modify Recipient

Message Type: O&M messages | TEST

Recipient: Add Recipient

□	Name	Phone Number	Email Address	Description
□	1[redacted]	+86 123***... Unverified	--	--
□	1[redacted]	+86 123***... Unverified	1*****@****... Unverified	--

NOTE

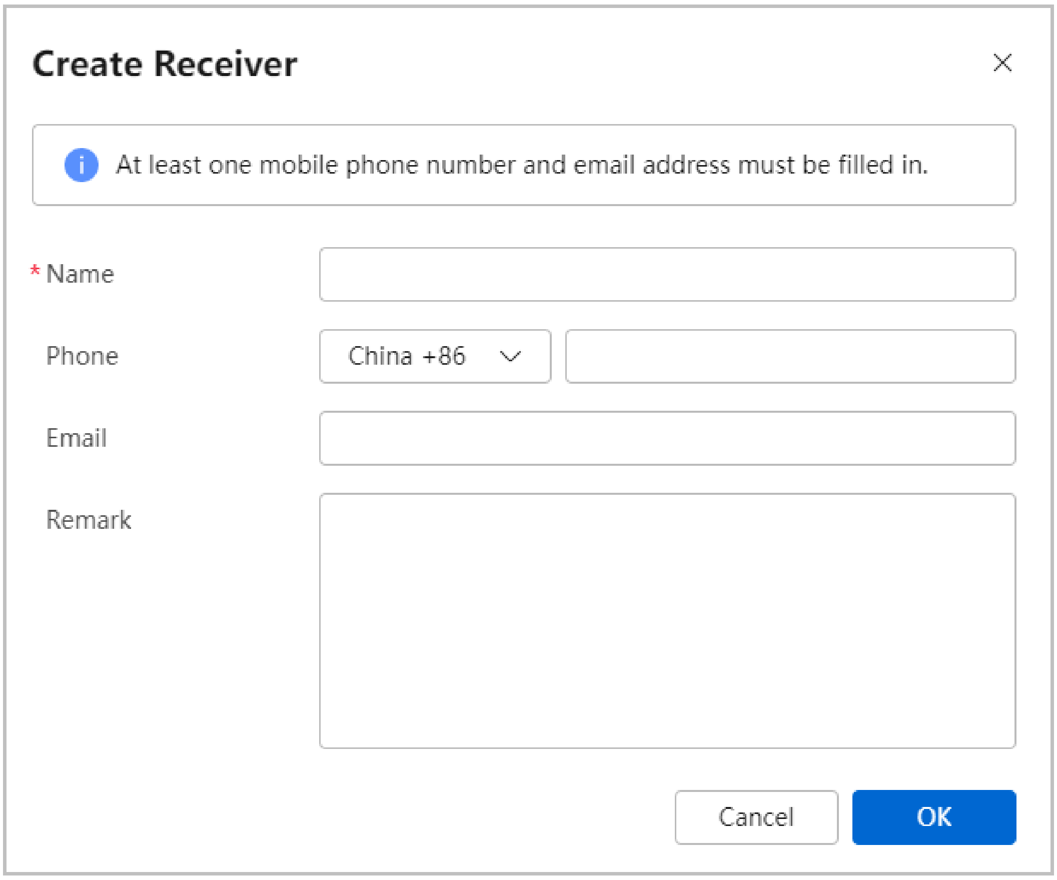
- If the **admin** user has uploaded a message sample during message type configuration, the **Preview** button is displayed in the **Operation** column of the message list.
- If the **admin** user has configured that messages of a certain type will be sent via email or SMS, the **Modify Receiver** button is displayed in the **Operation** column of the message type list.

4. Manage recipients.

a. Choose **Message Receiving Management** > **Recipient Management**. On the **Recipient Management** page, click **Create**.

b. Enter the name, phone number, and email address of a recipient, and click **OK**.

Figure 17-2 Creating a recipient



Create Receiver

At least one mobile phone number and email address must be filled in.

* Name

Phone China +86

Email

Remark

NOTE

Enter a phone number, email address, or both.

c. After the recipient is created, hover the mouse pointer over **Unverified** next to the phone number or email address, and click **Send Verification Link**. Only after being verified, the phone or email address can receive notifications.

NOTE

- Ensure that **SMS** or **Email** is selected for a recipient so that the recipient can receive SMS or email notifications.
- A login account can create a maximum of 20 recipients.

Follow-up Procedure

Manage recipients.

- Search: Enter a recipient name in the search box, and click 🔍 on the left or press **Enter** to search for the recipient.
- Configure message receiving: Click **Configure Message Receiving** in the **Operation** column to set the type of messages that the current recipient can receive.
- Modify recipient information: Click **Modify** in the recipient list to modify recipient information, including the name, phone number, and email address.

- Delete a recipient.
  - To delete a single recipient, click **Delete** in the **Operation** column of the recipient to delete.
  - To delete recipients in batches, select the recipients and click **Delete** in the upper right corner of the recipient list.

18 FAQs

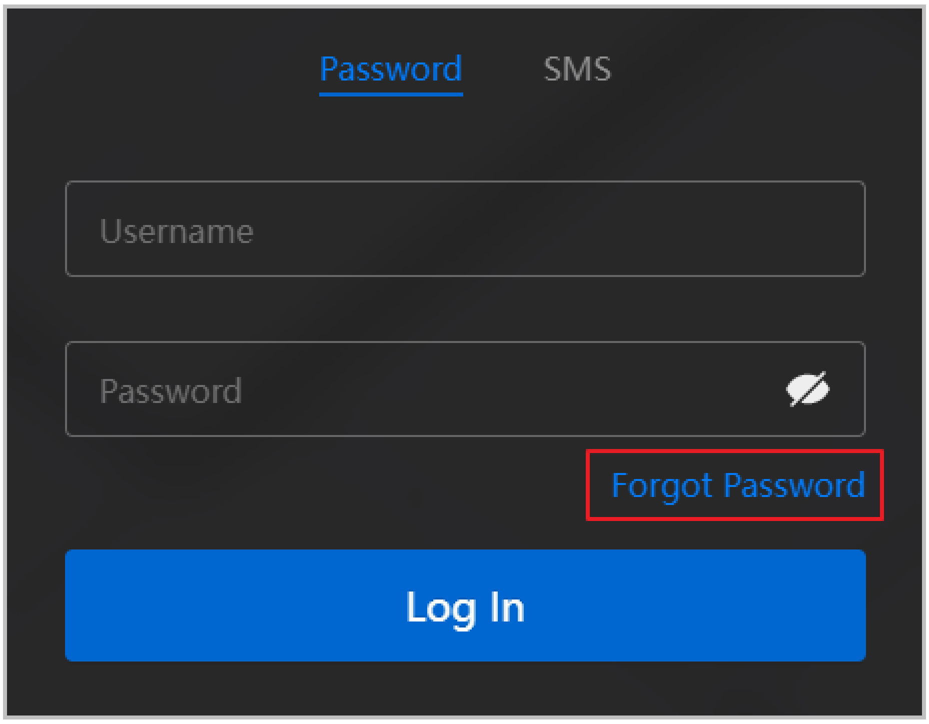
18.1 What Do I Do If I Forget the Console Login Password?

You can retrieve your password of your Huawei Qiankun account only if you have linked a phone number or email address to your account.

To retrieve your password, perform the following operations:

1. Access the Huawei Qiankun **console**.
2. Click **Forgot Password**.

Figure 18-1 Console login page



3. Enter your username and complete security verification.
4. Enter the linked phone number or email address for identity authentication.
5. After successful verification, reset the password. The new password must meet the **password requirements**.

18.2 Do I Need to Change My Password Periodically?

For your account security purposes, you are advised to change your password periodically, regardless of whether your account is created by yourself or another user.

By default, the validity period of a password is 90 days. Ten days before a password expires, the system prompts you to change the password upon your login. If you have linked an email address to your account, the system also sends a password expiration notification email to you every day until you change the password. For details, see **Changing User Passwords**.

For details, see **Password Change**.

18.3 How Do I View the Cloud Service Product Documentation on the Console?

To view the service introduction and user guide of Huawei Qiankun CloudService, click the online help icon ? in the menu bar.

18.4 How Do I View the Latest Service Notices?

You can learn about the latest news of Huawei Qiankun, such as new products and system upgrades, in the following ways:

- Click **Qiankun** in the upper left corner of the console. In the **Notice** area, click **Product Notice** to view the notice details.
- Click your account in the upper right corner of the console and click **Notices**.